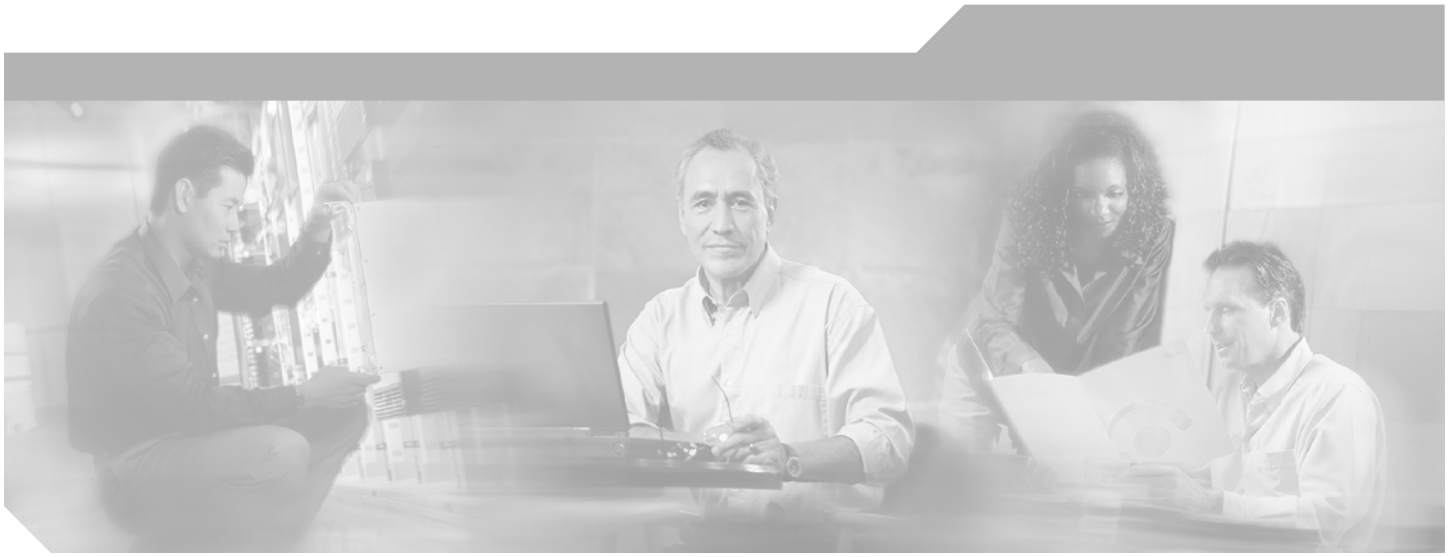


Cisco Aironet 1100 Series Access Point Hardware Installation Guide

December 2006

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-4309-07

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco Aironet 1100 Series Access Point Hardware Installation Guide

CONTENTS

Preface

Audience

This guide is for the networking professional who installs and manages the Cisco Aironet 1100 Series Access Point. The 1100 series access point is available in autonomous and lightweight configurations.

To use this guide with autonomous access points, you should have experience working with Cisco IOS software and be familiar with the concepts and terminology of wireless local area networks.

To use this guide with lightweight access points, you should have experience working with a Cisco Wireless LAN Controller and be familiar with the concepts and terminology of wireless local area networks.

Purpose

This guide provides the information you need to install your autonomous or lightweight access point.

For detailed information about Cisco IOS commands used with autonomous access points, refer to the *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges* for this release. For information about the standard Cisco IOS Release 12.3 commands, refer to the Cisco IOS documentation set available from the Cisco.com home page at **Technical Support & Documentation**. On the Technical Support & Documentation home page, click **Cisco IOS Software > Cisco IOS Software Releases 12.3 Mainline**.

For information about Cisco Wireless LAN Controllers, refer to the Cisco documentation sets available from the Cisco.com home page at **Technical Support & Documentation**. On the Technical Support & Documentation home page, click **Wireless** and the documentation is listed under the "Wireless LAN Controllers" section.

Organization

This guide is organized into these chapters:

Chapter 1, "Overview," lists the software and hardware features of the access point and describes the access point's role in your network.

Chapter 2, "Installing the Access Point," describes how to connect Ethernet and power cables and provides an installation summary, safety warnings, and general guidelines.

Chapter 3, "Mounting Instructions," describes how to mount the access point on a desktop, wall, or ceiling.

Chapter 4, "2.4-GHz Radio Upgrade for Autonomous Access Points," provides upgrade instructions for changing the 2.4 GHz radio

Chapter 5, "Troubleshooting Autonomous Access Points," provides troubleshooting procedures for basic problems with the autonomous access point.

Chapter 6, "Troubleshooting Lightweight Access Points," provides troubleshooting procedures for basic problems with the lightweight access point.

Appendix A, "Translated Safety Warnings,"indicates how to access the document that provides translations of the safety warnings that appear in this publication.

Appendix B, "Declarations of Conformity and Regulatory Information," provides declarations of conformity and regulatory information for the access point.

Appendix C, "Access Point Specifications," lists technical specifications for the access point.

Appendix D, "Channels and Maximum Power Levels," indicates how to access the document that lists the access point radio channels and the maximum power levels supported by the world's regulatory domains.

Appendix E, "Priming Lightweight Access Points Prior to Deployment," describes the procedure to prime lightweight access points with controller information.

Appendix F, "Configuring DHCP Option 43 for Lightweight Access Points," describes the procedure to configure DHCP Option 43 for lightweight access points.

Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in boldface text.
- Arguments for which you supply values are in italic.
- Square brackets ([ ]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in `screen` font.
- Information you enter is in **`boldface screen`** font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes, cautions, and timesavers use these conventions and symbols:

Tip Means the following will help you solve a problem. The tips information might not be troubleshooting or even an action, but could be useful information.

Note Means reader take note. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means reader be careful. In this situation, you might do something that could result equipment damage or loss of data.

Warning **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. (To see translations of the warnings that appear in this publication, refer to the appendix "Translated Safety Warnings.")**

Waarschuwing **Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van standaard maatregelen om ongelukken te voorkomen. (Voor vertalingen van de waarschuwingen die in deze publicatie verschijnen, kunt u het aanhangsel "Translated Safety Warnings" (Vertalingen van veiligheidsvoorschriften) raadplegen.)**

Varoitus **Tämä varoitusmerkki merkitsee vaaraa. Olet tilanteessa, joka voi johtaa ruumiinvammaan. Ennen kuin työskentelet minkään laitteiston parissa, ota selvää sähkökytkentöihin liittyvistä vaaroista ja tavanomaisista onnettomuuksien ehkäisykeinoista. (Tässä julkaisussa esiintyvien varoitusten käännökset löydät liitteestä "Translated Safety Warnings" (käännetyt turvallisuutta koskevat varoitukset).)**

Attention **Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures. Avant d'accéder à cet équipement, soyez conscient des dangers posés par les circuits électriques et familiarisez-vous avec les procédures courantes de prévention des accidents. Pour obtenir les traductions des mises en garde figurant dans cette publication, veuillez consulter l'annexe intitulée « Translated Safety Warnings » (Traduction des avis de sécurité).**

Warnung **Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu einer Körperverletzung führen könnte. Bevor Sie mit der Arbeit an irgendeinem Gerät beginnen, seien Sie sich der mit elektrischen Stromkreisen verbundenen Gefahren und der Standardpraktiken zur Vermeidung von Unfällen bewußt. (Übersetzungen der in dieser Veröffentlichung enthaltenen Warnhinweise finden Sie im Anhang mit dem Titel "Translated Safety Warnings" (Übersetzung der Warnhinweise).)**

Avvertenza **Questo simbolo di avvertenza indica un pericolo. Si è in una situazione che può causare infortuni. Prima di lavorare su qualsiasi apparecchiatura, occorre conoscere i pericoli relativi ai circuiti elettrici ed essere al corrente delle pratiche standard per la prevenzione di incidenti. La traduzione delle avvertenze riportate in questa pubblicazione si trova nell'appendice, "Translated Safety Warnings" (Traduzione delle avvertenze di sicurezza).**

Advarsel **Dette varselsymbolet betyr fare. Du befinner deg i en situasjon som kan føre til personskade. Før du utfører arbeid på utstyr, må du være oppmerksom på de faremomentene som elektriske kretser innebærer, samt gjøre deg kjent med vanlig praksis når det gjelder å unngå ulykker. (Hvis du vil se oversettelser av de advarslene som finnes i denne publikasjonen, kan du se i vedlegget "Translated Safety Warnings" [Oversatte sikkerhetsadvarsler].)**

Aviso **Este símbolo de aviso indica perigo. Encontra-se numa situação que lhe poderá causar danos fisicos. Antes de começar a trabalhar com qualquer equipamento, familiarize-se com os perigos relacionados com circuitos eléctricos, e com quaisquer práticas comuns que possam prevenir possíveis acidentes. (Para ver as traduções dos avisos que constam desta publicação, consulte o apêndice "Translated Safety Warnings" - "Traduções dos Avisos de Segurança").**

¡Advertencia! **Este símbolo de aviso significa peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considerar los riesgos que entraña la corriente eléctrica y familiarizarse con los procedimientos estándar de prevención de accidentes. (Para ver traducciones de las advertencias que aparecen en esta publicación, consultar el apéndice titulado "Translated Safety Warnings.")**

Varning! **Denna varningssymbol signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanligt förfarande för att förebygga skador. (Se förklaringar av de varningar som förekommer i denna publikation i appendix "Translated Safety Warnings" [Översatta säkerhetsvarningar].)**

Related Publications

These documents provide information about the autonomous access point:

- Release Notes for Cisco Aironet 1100 Series Access Points
- *Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges*
- *CCisco IOS Software Configuration Guide for Cisco Aironet Access Points*

These documents provide information about the lightweight access point and the controller:

- *Release Notes for Cisco Aironet 1100 Series Access Points*
- *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*

Click this link to browse to the Cisco Wireless documentation home page:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

To browse to the 1100 series access point documentation, click **Cisco Aironet 1100 Series** listed under "Wireless LAN Access."

To browse to the Cisco Wireless LAN Controller documentation, click **Cisco 4400 Series Wireless LAN Controllers** or **Cisco 2000 Series Wireless LAN Controllers** listed under "Wireless LAN Controllers."

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. This section explains the product documentation resources that Cisco offers.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Product Documentation DVD

The Product Documentation DVD is a library of technical product documentation on a portable medium. The DVD enables you to access installation, configuration, and command guides for Cisco hardware and software products. With the DVD, you have access to the HTML documentation and some of the PDF files found on the Cisco website at this URL:

http://www.cisco.com/univercd/home/home.htm

The Product Documentation DVD is created and released regularly. DVDs are available singly or by subscription. Registered Cisco.com users can order a Product Documentation DVD (product number DOC-DOCDVD= or DOC-DOCDVD=SUB) from Cisco Marketplace at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

Ordering Documentation

You must be a registered Cisco.com user to access Cisco Marketplace. Registered users may order Cisco documentation at the Product Documentation Store at this URL:

http://www.cisco.com/go/marketplace/docstore

If you do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Documentation Feedback

You can provide feedback about Cisco technical documentation on the Cisco Support site area by entering your comments in the feedback form available in every online document.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you will find information about how to do the following:

- Report security vulnerabilities in Cisco products

- Obtain assistance with security incidents that involve Cisco products
- Register to receive security information from Cisco

A current list of security advisories, security notices, and security responses for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

To see security advisories, security notices, and security responses as they are updated in real time, you can subscribe to the Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed. Information about how to subscribe to the PSIRT RSS feed is found at this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you have identified a vulnerability in a Cisco product, contact PSIRT:

- For emergencies only—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.
- For nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product (for example, GnuPG) to encrypt any sensitive information that you send to Cisco. PSIRT can work with information that has been encrypted with PGP versions 2.*x* through 9.*x*.

Never use a revoked encryption key or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

The link on this page has the current PGP key ID in use.

If you do not have or use PGP, contact PSIRT to find other means of encrypting the data before sending any sensitive material.

Product Alerts and Field Notices

Modifications to or updates about Cisco products are announced in Cisco Product Alerts and Cisco Field Notices. You can receive these announcements by using the Product Alert Tool on Cisco.com. This tool enables you to create a profile and choose those products for which you want to receive information.

To access the Product Alert Tool, you must be a registered Cisco.com user. Registered users can access the tool at this URL:

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

To register as a Cisco.com user, go to this URL:

http://tools.cisco.com/RPF/register/register.do

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Support website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Support Website

The Cisco Support website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day at this URL:

http://www.cisco.com/en/US/support/index.html

Access to all tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Before you submit a request for service online or by phone, use the **Cisco Product Identification Tool** to locate your product serial number. You can access this tool from the Cisco Support website by clicking the **Get Tools & Resources** link, clicking the **All Tools (A-Z)** tab, and then choosing **Cisco Product Identification Tool** from the alphabetical list. This tool offers three search options: by product ID or model name; by tree view; or, for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Tip **Displaying and Searching on Cisco.com**

If you suspect that the browser is not refreshing a web page, force the browser to update the web page by holding down the Ctrl key while pressing **F5**.

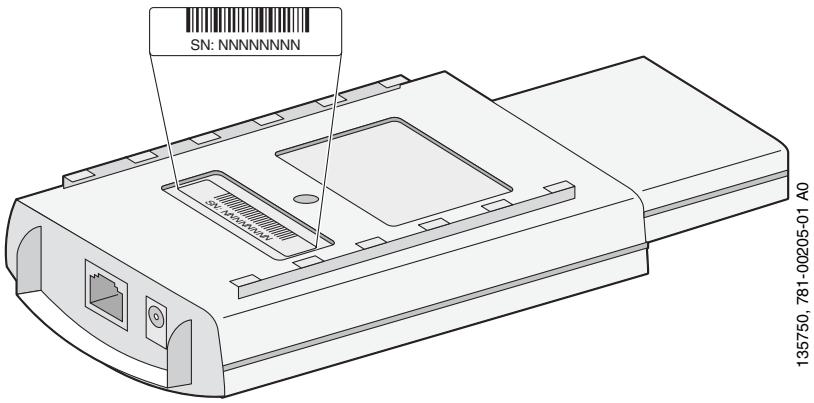
To find technical information, narrow your search to look in technical documentation, not the entire Cisco.com website. After using the Search box on the Cisco.com home page, click the **Advanced Search** link next to the Search box on the resulting page and then click the **Technical Support & Documentation** radio button.

To provide feedback about the Cisco.com website or a particular technical document, click **Contacts & Feedback** at the top of any Cisco.com web page.

Locating the Product Serial Number

The access point serial number is located on the back of the housing (refer to Figure 1).

Figure 1 Location of Serial Number Label



The access point serial number label contains the following information:

- Model number, such as *AIR-AP1100* or *AIR-LAP1100*
- Serial number, such as S/N: *VDF0636XXXX* (11 alphanumeric digits)
- MAC address, such as MAC: *00abc65094f3* (12 hexadecimal digits)
- Location of manufacture, such as *Made in Singapore*

You need your product serial number when requesting support from the Cisco Technical Assistance Center.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests, or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411
Australia: 1 800 805 227
EMEA: +32 2 704 55 55
USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—An existing network is “down” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of the network is impaired while most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The Cisco Online Subscription Center is the website where you can sign up for a variety of Cisco e-mail newsletters and other communications. Create a profile and then select the subscriptions that you would like to receive. To visit the Cisco Online Subscription Center, go to this URL:

  http://www.cisco.com/offer/subscribe

- The *Cisco Product Quick Reference Guide* is a handy, compact reference tool that includes brief product overviews, key features, sample part numbers, and abbreviated technical specifications for many Cisco products that are sold through channel partners. It is updated twice a year and includes the latest Cisco channel product offerings. To order and find out more about the *Cisco Product Quick Reference Guide*, go to this URL:

  http://www.cisco.com/go/guide

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- Cisco Press publishes a wide range of general networking, training, and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Internet Protocol Journal* is a quarterly journal published by Cisco for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the *Internet Protocol Journal* at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco, as well as customer support services, can be obtained at this URL:

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection is an interactive website where networking professionals share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- "What's New in Cisco Documentation" is an online publication that provides information about the latest documentation releases for Cisco products. Updated monthly, this online publication is organized by product category to direct you quickly to the documentation for your products. You can view the latest release of "What's New in Cisco Documentation" at this URL:

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Overview

The Cisco Aironet Cisco Aironet 1100 Series Access Point series access point is available in autonomous and lightweight configurations. The autonomous access points can support standalone network configurations with all configuration settings maintained within the access points. The lightweight access points operate in conjunction with a Cisco wireless LAN controller with all configuration information maintained within the controller.

Product Terminology

The following terms refer to the autonomous and lightweight products:

- The term *access point* describes both autonomous and lightweight products.
- The term *autonomous access point* describes only the autonomous product.
- The term *lightweight access point* describs only the lightweight product.
- The term *access point* describes the product when configured to operate as an access point.
- The term *bridge* describes the product when configured to operate as a bridge.

Autonomous Access Points

The autonomous access point (models: AIR-AP1120B or AIR-AP1121G) (model: AIR-AP1252) supports a management system based on Cisco IOS software. The 1100 series is a Wi-Fi certified, wireless LAN transceiver and uses a single mini-PCI radio (IEEE 802.11b-compliant or IEEE 802.11g-compliant).

The access point serves as the connection point between wireless and wired networks or as the center point of a stand-alone wireless network. In large installations, wireless users within radio range of an access point can roam throughout a facility while maintaining seamless access to the network.

You can configure and monitor the access point using the command-line interface (CLI), the browser-based management system, or Simple Network Management Protocol (SNMP).

Lightweight Access Points

The Cisco Aironet 1100 Series Lightweight Access Point (AIR-LAP1121G) is part of the Cisco Integrated Wireless Network Solution and requires no manual configuration before being mounted. The lightweight access point is automatically configured by a Cisco wireless LAN controller (hereafter called a *controller*) using the Lightweight Access Point Protocol (LWAPP).

The lightweight access point contains one integrated radio: a 2.4-GHz radio (IEEE 802.11g). Using a controller, you can configure the radio settings.

In the Cisco Centralized Wireless LAN architecture, access points operate in the lightweight mode (as opposed to autonomous mode). The lightweight access points associate to a controller. The controller manages the configuration, firmware, and controls transactions such as 802.1x authentication. In addition, all wireless traffic is tunneled through the controller.

LWAPP is an Internet Engineering Task Force (IETF) draft protocol that defines the control messaging for setup and path authentication and run-time operations. LWAPP also defines the tunneling mechanism for data traffic.

In an LWAPP environment, a lightweight access point discovers a controller by using LWAPP discovery mechanisms and then sends it an LWAPP join request. The controller sends the lightweight access point an LWAPP join response allowing the access point to join the controller. When the access point is joined, the access point downloads its software if the versions on the access point and controller do not match. After an access point joins a controller, you can reassign it to any controller on your network.

LWAPP secures the control communication between the lightweight access point and controller by means of a secure key distribution, using X.509 certificates on both the access point and controller.

This chapter provides information on the following topics:

Hardware Features

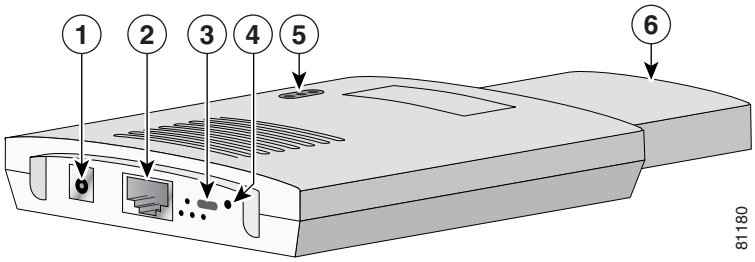
This section describes the access point features. Refer to Appendix C, "Access Point Specifications," for a list of access point specifications.

Key hardware features of the 1100 series access point include:

- Single Radio Operation, page 1-3
- Ethernet Port, page 1-3
- LEDs, page 1-4
- Power Sources, page 1-4
- UL 2043 Certification, page 1-5
- Anti-Theft Features, page 1-5

Figure 1-1 shows the location of some of the hardware features of the access point.

Figure 1-1 Access Point Layout and Connectors



1	48-VDC power port	**4**	Mode button
2	Ethernet port (RJ-45)	**5**	Status LEDs
3	Cable lock slot	**6**	Antenna

Single Radio Operation

The access point contains a 2.4-GHz radio (IEEE 802.11b-compliant or IEEE 802.11g-compliant) in a mini-PCI slot and two 2.2-dBi dipole integrated antennas. You can perform a field upgrade to the mini-PCI radio and antennas to support new radio technologies, such as the 2.4-GHz IEEE 802.11g-compliant radio.

Ethernet Port

The auto-sensing Ethernet port accepts an RJ-45 connector, linking the access point to your 10BASE-T or 100BASE-T Ethernet LAN. The access point can receive power through the Ethernet cable from a power injector, switch, or power patch panel. The Ethernet MAC address is printed on the label on the back of the access point.

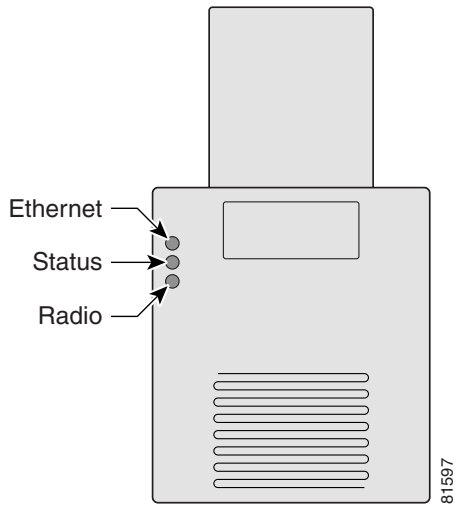
LEDs

The three LEDs on the top of the access point report Ethernet activity, association status, and radio activity.

- The Ethernet LED signals Ethernet traffic on the wired LAN, or Ethernet infrastructure. This LED is normally green when an Ethernet cable is connected, and blinks green when a packet is received or transmitted over the Ethernet infrastructure. The LED is off when the Ethernet cable is not connected.
- The status LED signals operational status. Steady green indicates that the access point is associated with at least one wireless client. Blinking green indicates that the access point is operating normally but is not associated with any wireless devices.
- The radio LED signals wireless traffic over the radio interface. The light is normally off, but it blinks green whenever a packet is received or transmitted over the access point radio.

Figure 1-2 shows the three status LEDs.

Figure 1-2 Access Point LEDs



Power Sources

The access point draws up to 4.9W of DC power and can receive power from an external power module or through inline power using the Ethernet cable. Using inline power, you do not need to run a separate power cord to the access point. The access point supports the following power sources:

- Power supply (input 100–240 VAC, 50–60 Hz, output 48 VDC, 0.2A minimum)
- Inline power from:
  - Cisco Aironet Power Injector (Cisco AIR-PWRINJ3= or Cisco AIR-PWRINJ-FIB=)
  - A switch capable of providing inline power, such as the Cisco Catalyst 3500XL, 3550, 4000, or 6500
  - An inline power patch panel, such as the Cisco Catalyst Inline Power Patch Panel

UL 2043 Certification

The access point is encased in a durable plastic enclosure having adequate fire resistance and low smoke-producing characteristics suitable for operation in a building's environmental air space, such as above suspended ceilings, in accordance with Section 300-22(c) of the NEC, and with Sections 2-128, 12-010(3) and 12-100 of the *Canadian Electrical Code*, Part 1, C22.1.

Caution Only the fiber-optic power injector (AIR-PWRINJ-FIB) has been tested to UL 2043 for operation in a building's environmental air space; no other power injectors or power modules have been tested to UL 2043 and they should not be placed in a building's environmental air space, such as above suspended ceilings.

Anti-Theft Features

There are two methods of securing the access point to help prevent theft:

- Security cable keyhole—You can use the security cable slot to secure the access point using a standard security cable, such as those used on laptop computers.
- Security hasp—When you mount the access point on a wall or ceiling using the mounting bracket and the security hasp, you can lock the access point to the bracket with a padlock. Compatible padlocks are Master Lock models 120T and 121T or equivalent.

Network Examples with Autonomous Access Points

This section describes the autonomous access point's role in three common wireless network configurations. The autonomous access point's default configuration is as a root unit connected to a wired LAN or as the central unit in an all-wireless network. The repeater role requires a specific configuration.

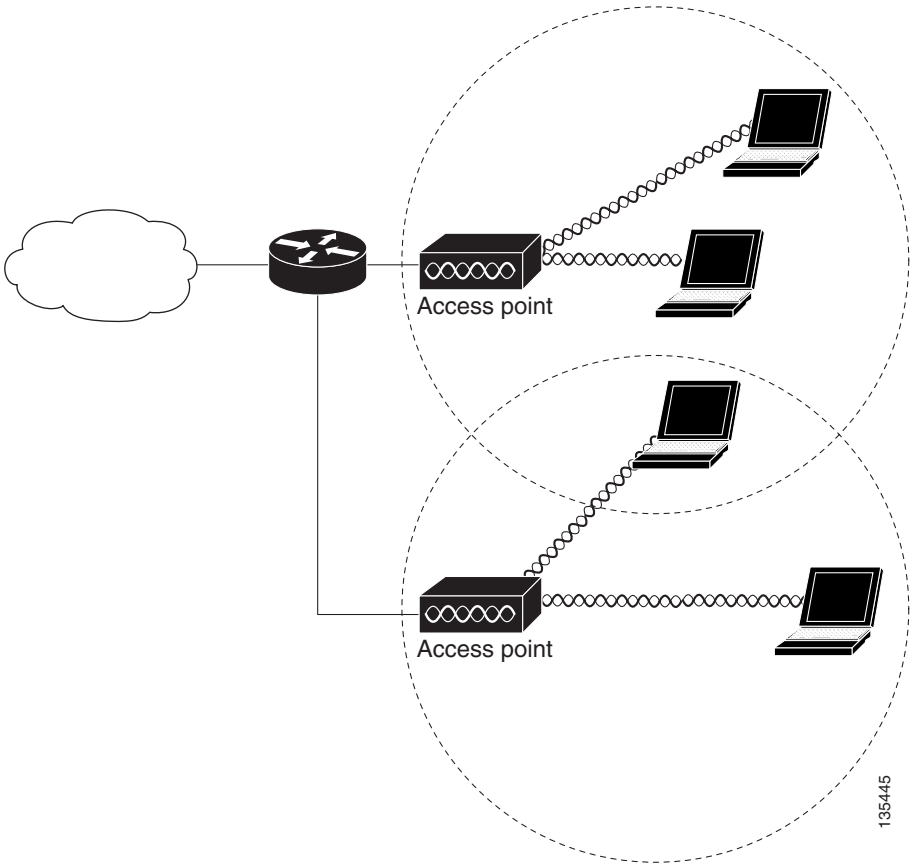
The autonomous 1100 series access point supports these operating wireless modes:

- Root access point—Connected to a wired LAN and supports wireless clients.
- Repeater access point—Not connected to a wired LAN, associates to a root access point, and supports wireless clients
- Workgroup bridge—Not connected to a wired LAN, associates to a root access point or bridge, and supports wired network devices.

Root Unit on a Wired LAN

An autonomous access point connected directly to a wired LAN provides a connection point for wireless users. If more than one autonomous access point is connected to the LAN, users can roam from one area of a facility to another without losing their connection to the network. As users move out of range of one access point, they automatically connect to the network (associate) through another access point. The roaming process is seamless and transparent to the user. Figure 1-3 shows access points acting as root units on a wired LAN.

Figure 1-3 Access Points as Root Units on a Wired LAN

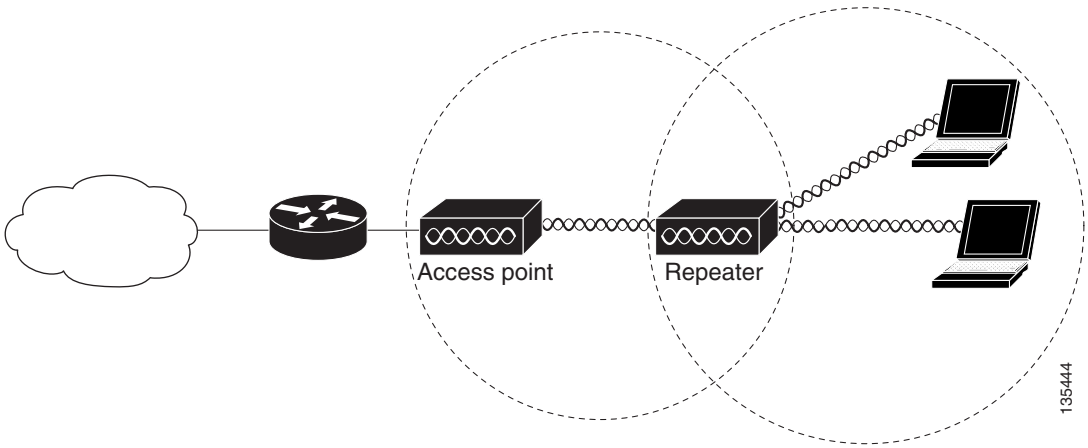


Repeater Unit that Extends Wireless Range

An autonomous access point can be configured as a stand-alone repeater to extend the range of your infrastructure or to overcome an obstacle that blocks radio communication. The repeater forwards traffic between wireless users and the wired LAN by sending packets to either another repeater or to an access point connected to the wired LAN. The data is sent through the route that provides the best performance for the client. Figure 1-4 shows an autonomous access point acting as a repeater. Consult the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for instructions on setting up an access point as a repeater.

Note Non-Cisco client devices might have difficulty communicating with repeater access points.

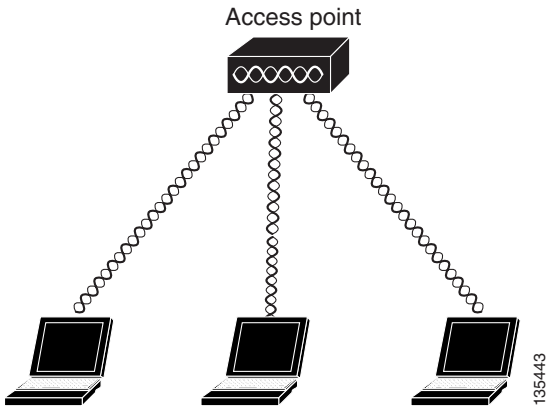
Figure 1-4 Access Point as Repeater



Central Unit in an All-Wireless Network

In an all-wireless network, an autonomous access point acts as a stand-alone root unit. The autonomous access point is not attached to a wired LAN; it functions as a hub linking all stations together. The access point serves as the focal point for communications, increasing the communication range of wireless users. Figure 1-5 shows an autonomous access point in an all-wireless network.

Figure 1-5 Access Point as Central Unit in All-Wireless Network

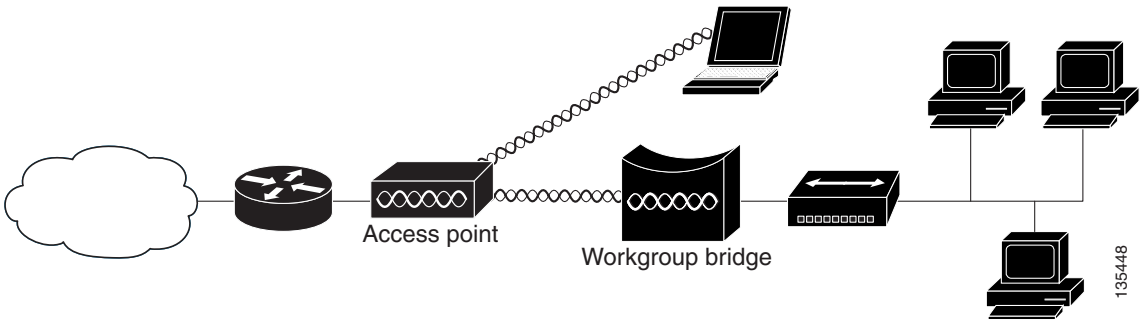


Workgroup Bridge Configuration

When configured in the workgroup bridge mode, the autonomous unit provides a wireless connection for remote wired devices to a Cisco Aironet access point or to a Cisco Aironet bridge.

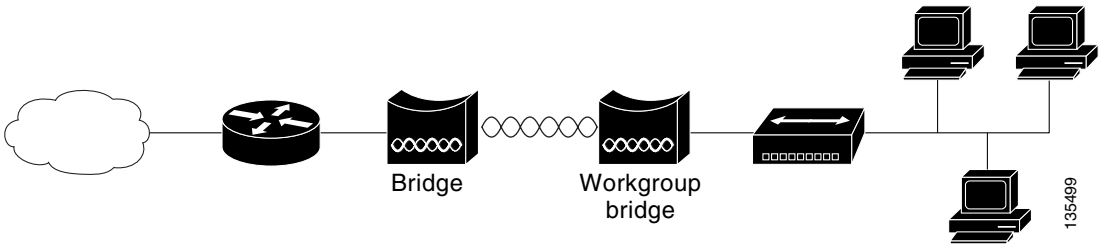
In Figure 1-6, the unit is configured in workgroup bridge mode and is associated to a Cisco Aironet access point as a wireless client device. This configuration allows the Ethernet-enabled devices to pass Ethernet traffic to and from the main LAN using the workgroup bridge.

Figure 1-6 Workgroup Bridge Configuration 1



In Figure 1-7, the autonomous unit is configured in workgroup bridge mode and is associated to a Cisco Aironet root bridge as a wireless bridge device. This configuration allows the Ethernet-enabled devices pass Ethernet traffic to and from the main LAN using the workgroup bridge. The main advantage of this configuration is that the wireless communication link can be over a longer distance than an access point supports. Typically, an access point can communicate over approximately a 1-mile range; however, the bridge-to-bridge wireless link can communicate over approximately a 21-mile range.

Figure 1-7 Workgroup Bridge Configuration 2

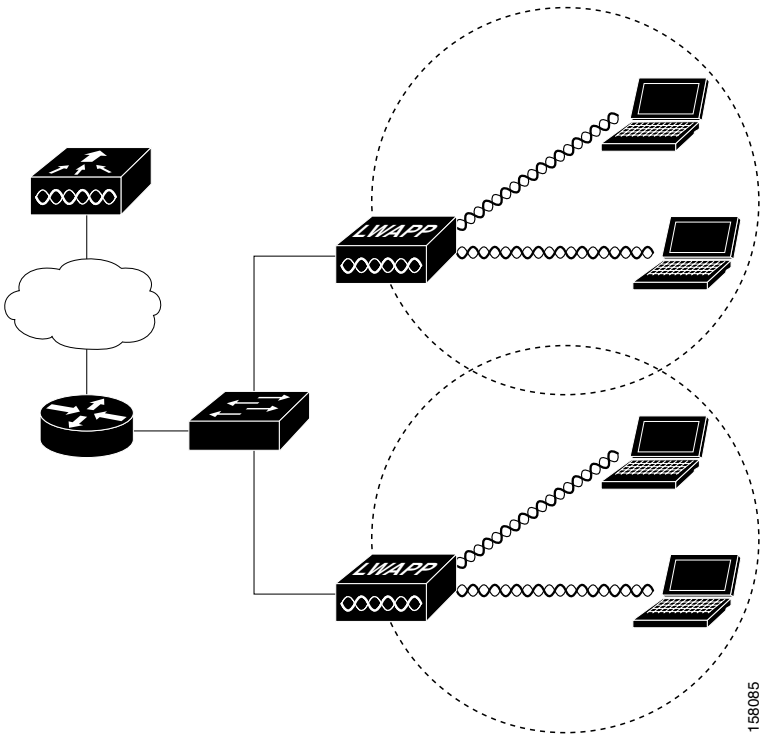


Network Example with Lightweight Access Points

The lightweight access points support Layer 3 network operation. Lightweight access points and controllers in Layer 3 configurations use IP addresses and UDP packets, which can be routed through large networks. Layer 3 operation is scalable and recommended by Cisco.

Figure 1-8 illustrates a typical Layer 3 network configuration containing lightweight access points.

Figure 1-8 Typical Layer 3 Network Configuration Example



CHAPTER 2

Installing the Access Point

This chapter describes the setup of the access point and includes the following sections:

Safety Information

Follow the guidelines in this section to ensure proper operation and safe use of the access point.

FCC Safety Compliance Statement

The FCC with its action in ET Docket 96-8 has adopted a safety standard for human exposure to radio frequency (RF) electromagnetic energy emitted by FCC certified equipment. When used with approved Cisco Aironet antennas, Cisco Aironet products meet the uncontrolled environmental limits found in OET-65 and ANSI C95.1, 1991. Proper installation of this radio according to the instructions found in this manual will result in user exposure that is substantially below the FCC recommended limits.

General Safety Guidelines

- Do not touch or move antenna(s) while the unit is transmitting or receiving.
- Do not hold any component containing a radio so that the antenna is very close to or touching any exposed parts of the body, especially the face or eyes, while transmitting.
- The use of wireless devices in hazardous locations is limited to the constraints posed by the local codes, the national codes, and the safety directors of such environments.

Warnings

Translated versions of all safety warnings are available in the safety warning document that shipped with your access point or on Cisco.com. To browse to the document on Cisco.com, refer to Appendix A, "Translated Safety Warnings" for instructions.

Warning **Do not operate your wireless network device near unshielded blasting caps or in an explosive environment unless the device has been modified to be especially qualified for such use.** Statement 245B

Warning **In order to comply with FCC radio frequency (RF) exposure limits, antennas should be located at a minimum of 7.9 inches (20 cm) or more from the body of all persons.** Statement 332

Warning **Do not work on the system or connect or disconnect cables during periods of lightning activity.** Statement 1001

Warning **Read the installation instructions before you connect the system to its power source.** Statement 1004

Warning **This product relies on the building's installation for short-circuit (overcurrent) protection. Ensure that the protective device is rated not greater than: 20 A..** Statement 1005

Unpacking the Access Point

Follow these steps to unpack the access point:

Step 1 Open the shipping container and carefully remove the contents.

Step 2 Return all packing materials to the shipping container and save it.

Step 3 Ensure that all items listed in the "Package Contents" section are included in the shipment. Check each item for damage. If any item is damaged or missing, notify your authorized Cisco sales representative.

Package Contents

Each access point package contains the following items:

- Access point with power module
- Wall or ceiling mounting bracket
- Security hasp adapter
- Cubical partition mounting bracket assembly
- Horizontal surface mounting holster
- Mounting hardware kit
- Product quick start quide
- Product safety warnings document
- Cisco product registration and Cisco documentation feedback cards

Basic Installation Guidelines

Because the access point is a radio device, it is susceptible to interference that can reduce throughput and range. Follow these basic guidelines to ensure the best possible performance:

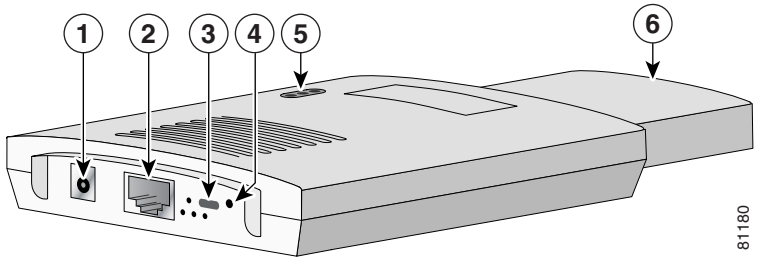
- Ensure a site survey has been performed to determine the optimum placement of access points.
- For lightweight access points, check the latest release notes to ensure that your controller software version supports the access points to be installed. You can find the controller release notes by selecting your controller under **Wireless LAN Controllers** at this URL:

  http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html
- Ensure that access points are not mounted closer than 20 cm (7.9 in) from the body of all persons.
- Do not mount the access point within 3 feet of metal obstructions.
- Install the access point away from microwave ovens. Microwave ovens operate on the same frequency as the access point and can cause signal interference.
- Do not mount the access point outside of buildings.
- Do not mount the access points on building perimeter walls unless outside coverage is desired.

Access Point Layout and Connectors

Figure 2-1 shows the access point layout and connectors.

Figure 2-1 Access Point Layout and Connectors



1	48-VDC power port	**4**	Mode button
2	Ethernet port (RJ-45)	**5**	Status LEDs
3	Cable lock slot	**6**	Antenna

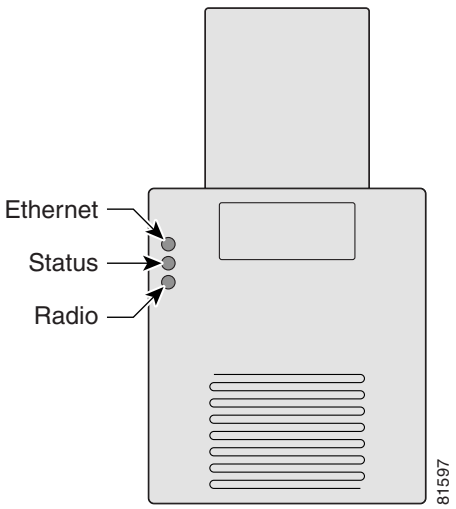
LEDs

The three LEDs on the top of the access point report Ethernet activity, association status, and radio activity.

- The Ethernet LED signals Ethernet traffic on the wired LAN.
- The status LED signals operational status.
- The radio LED signals wireless traffic over the radio interface.

Figure 2-2 shows the three status LEDs.

Figure 2-2 Access Point LEDs



Controller Discovery Process for Lightweight Access Points

The lightweight access point supports these controller discovery processes:

- DHCP server discovery—Uses DHCP Option 43 to provide controller IP addresses to the access points. Cisco switches support a DHCP server option. For additional information, refer to the "Configuring DHCP Option 43 for Lightweight Access Points" section on page F-1.
- DNS server discovery—The access point uses the name *CISCO-LWAPP-CONTROLLER.<local domain>* to discover the controller IP addresses from a DNS server. Where *<local domain>* is the access point domain name.
- Locally stored controller IP addresses—If the access point was previously associated to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point non-volatile memory. The process of storing controller IP addresses in access points for later deployment is called priming the access point. For additional information, refer to the "Priming Lightweight Access Points Prior to Deployment" section on page E-1.

For lightweight access points, Cisco recommends that you configure a DHCP server with Option 43 to provide the controller IP addresses to your access points. Cisco switches provide a DHCP server option that is typically used for this purpose.

Deploying the Access Points on the Wireless Network

Prior to beginning the actual access point deployment, perform these tasks:

- Ensure that a site survey has been preformed.
- Ensure that your network infrastructure devices are operational and properly configured.
- For lightweight access points, perform these tasks:
  - Ensure that your controllers are connected to switch trunk ports.
  - Ensure that your switch is configured with untagged access ports for connecting your access points.
  - Ensure that a DHCP server with Option 43 configured is reachable by your access points.

To deploy your access points, follow these steps:

Step 1 Obtain the access point location map created during your building site survey.

Step 2 Review the access point locations and identify the specific mounting methods required for each access point location.

Step 3 For each access point perform these steps:

a. For lightweight access points, record the access point MAC address on the access point location map. When you have completed the access point deployment, return the access point MAC addresses and the access point locations on the access point location maps or floor plans to your network planner or manager. The network operators can use the MAC address and location information to create maps for precise wireless system management.

b. Mount the access point at the indicated destination using the specified mounting method. For specific instructions, see these sections:
   - Horizontal or vertical surface, such as a ceiling or wall (refer to the Mounting on a Horizontal or Vertical Surface, page 3-3).
   - Below a suspended ceiling (refer to the "Mounting on a Suspended Ceiling" section on page 3-4).
   - Above a suspended ceiling (refer to the "Mounting Above a Suspended Ceiling" section on page 3-6).
   - On a cubicle wall (refer to the "Mounting on a Cubical Wall Partition" section on page 3-8).
   - On a desktop (see the "Using the Desktop Holster" section on page 3-9).

c. Optionally secure the access point using a padlock or security cable (refer to the "Using the Security Hasp Adapter" section on page 3-7 and the "Using the Cable Lock Feature" section on page 3-11).

d. Connect the access point cables (Ethernet, optional power, optional antennas). For instructions see the "Connecting the Ethernet and Power Cables" section on page 2-7.

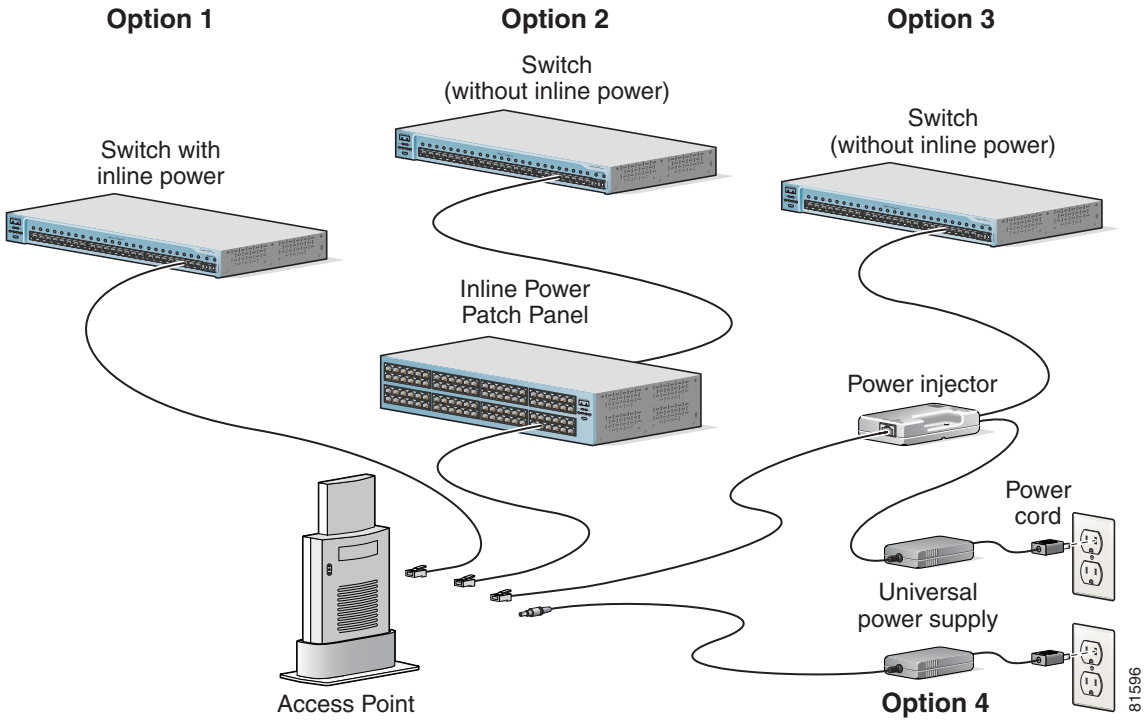
e. On power up, verify that the access point is operating normally by checking the LEDs. For additional information, refer to the "Checking the Autonomous Access Point LEDs" section on page 5-2 or the "Checking the Lightweight Access Point LEDs" section on page 6-3.

Step 4 For lightweight access points, after your access points are deployed, ensure that your controller is not configured as a master controller. A master controller should only be used for configuring access points and not in a working network.

Connecting the Ethernet and Power Cables

The access point receives power through the Ethernet cable or an external power module. Figure 2-3 shows the power options for the access point.

Figure 2-3 Access Point Power Options



The access point power options are listed below:

- A switch with inline power, such as a Cisco Catalyst 3500XL, 3550, 4000, or 6500 switch
- An inline power patch panel, such as a Cisco Catalyst Inline Power Patch Panel
- A power injector (Cisco AIR-PWRINJ3= or Cisco AIR-PWRINJ-FIB=)
- A power module (Universal power supply)

Note If you use in-line power from a switch or patch panel, do not connect the power module to the access point. Using two power sources on the access point might cause the switch or patch panel to shut down the port to which the access point is connected.

Connecting to an Ethernet Network with an Inline Power Source

Follow these steps to connect the access point to the Ethernet LAN when you have an inline power source:

Step 1 Connect the Ethernet cable to the RJ-45 Ethernet connector labeled *Ethernet* on the access point.

Step 2 Connect the other end of the Ethernet cable to one of the following:

- A switch with inline power, such as a Cisco Catalyst 3500XL, 3550, 4000, or 6500 switch.
- An inline power switch panel, such as a Cisco Catalyst Inline Power Patch Panel.
- The end of a Cisco Aironet power injector labeled *To AP/Bridge*. Connect the other end labeled *To Network* to the 10/100 Ethernet LAN.

Caution The Cisco Aironet Power Injector (Cisco AIR-PWRINJ3= or Cisco AIR-PWRINJ-FIB=) is designed for use with 1100 or 1200 series access points. Using the power injector with other Ethernet-ready devices can damage the equipment.

Caution Only the fiber-optic power injector (AIR-PWRINJ-FIB) has been tested to UL 2043 for operation in a building's environmental air space; no other power injectors or power modules have been tested to UL 2043 and they should not be placed in a building's environmental air space, such as above suspended ceilings.

Note If you use a power injector to power the access point, you must use the power supply included with your access point and the Cisco Aironet Power Injector specified for the access point.

Connecting to an Ethernet Network with Local Power

Follow these steps to connect the access point to an Ethernet LAN when you are using a local power source:

Step 1 Connect the Ethernet cable to the RJ-45 Ethernet connector labeled *Ethernet* on the access point.

Step 2 Plug the other end of the Ethernet cable into an unpowered Ethernet port on your network.

Step 3 Connect the power module's output connector to the 48-VDC power port labeled *48VDC* on the access point.

Step 4 Plug the other end of the power module into an approved 100- to 240-VAC outlet.

Powering Up the Access Point

When power is applied to the access point, it begins a routine power-up sequence that you can monitor by observing the three LEDs on top of the access point. After you observe all three LEDs turning green to indicate the starting of the Cisco IOS operating system, the Status LED blinks green signifying that Cisco IOS is operational. Refer to the "Checking the Autonomous Access Point LEDs" section on page 5-2 or the "Checking the Lightweight Access Point LEDs" section on page 6-3 for LED descriptions.

CHAPTER 3

Mounting Instructions

This appendix contains mounting instructions for the access point and contains the following topics:

Overview

The mounting brackets and hardware shipped with your access point enables you to mount it on any of the following surfaces:

- Horizontal or vertical flat surfaces, such as walls or ceilings
- Suspended ceilings
- Cubical partition walls
- Desktop or other suitable horizontal surface

The 1100 series access point provides adequate fire resistance and low smoke-producing characteristics suitable for operation in a building's environmental air space, such as above suspended ceilings, in accordance with Section 300-22(C) of the National Electrical Code (NEC) and Sections 2-128, 12-010(3) and 12-100 of the Canadian Electrical Code, Part 1, C22.1.

Caution Only the fiber-optic power injector (AIR-PWRINJ-FIB) has been tested to UL 2043 for operation in a building’s environmental air space; no other power injectors or power modules have been tested to UL 2043 and they should not be placed in a building’s environmental air space, such as above suspended ceilings.

Security features for each of these mounting methods are also provided. You can use a Kensington lock (Notebook Microstar, model number 64068), which you must provide, to make the access point more secure when you mount it using any of the mounting options.

You can use the security hasp adapter provided by Cisco to secure the access point with a padlock when you use the wall or ceiling mounting bracket. The security hasp adapter provides maximum physical security for your access point.

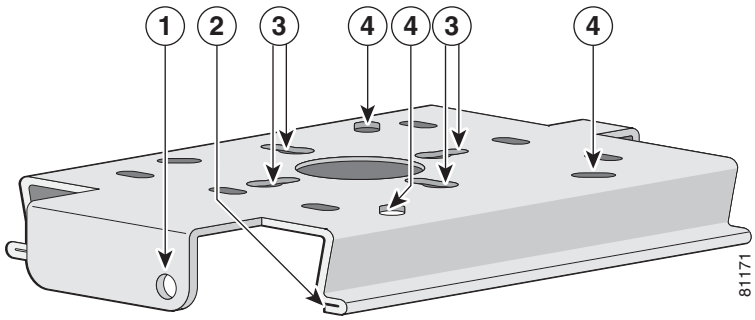
A mounting hardware kit is provided that contains the hardware and fasteners necessary to mount the access point. Refer to Table 3-1 to identify the materials you need to mount your access point, then go to the section containing the specific mounting procedure.

Table 3-1 Mounting Material

Mounting Method	Materials Required	In Kit
Horizontal or vertical surface	Wall or ceiling mounting bracket Security hasp adapter Four #8 x 1 in. (25.4 mm) screws Four wall anchors 3/16 in. (4.7 mm) or 3/32 in. (2.3 mm) drill bit Drill	Yes Yes Yes Yes No No
Suspended ceiling	Wall or ceiling mounting bracket Security hasp adapter Two caddy fasteners with studs Two plastic spacers Two 1/4–20 Keps nuts Standard screwdriver Appropriate wrench or pliers	Yes Yes Yes Yes Yes No No
Office cubical wall partition	Cubical partition mounting bracket assembly	Yes
Desktop	Desktop holster	Yes

The wall or ceiling mounting bracket also serves as a template for transferring the location of the bracket's mounting holes to the mounting surface. Refer to Figure 3-1 to locate the various mounting holes for the method you intend to use.

Figure 3-1 Mounting Bracket



1	Security hasp	**3**	Suspended ceiling mount holes
2	Access point mounting rail	**4**	Wall mount holes

Mounting on a Horizontal or Vertical Surface

Follow these steps to mount the access point on a horizontal or vertical surface, such as a ceiling or wall.

Step 1 Use the wall or ceiling mounting bracket as a template to mark the locations of the mounting holes.

- You can use any of the 10 holes around the periphery (three of which are identified in the illustration) of the bracket to mount it using the supplied #8 fasteners.

Step 2 Drill one of the following sized holes at the locations you marked:

- 3/16 in. (4.7 mm) if you are using wall anchors
- 3/32 in. (2.3 mm) if you are not using wall anchors

Step 3 Install the anchors into the wall if you are using them. Otherwise, go to Step 4.

Step 4 Secure the mounting bracket to the surface using the #8 fasteners.

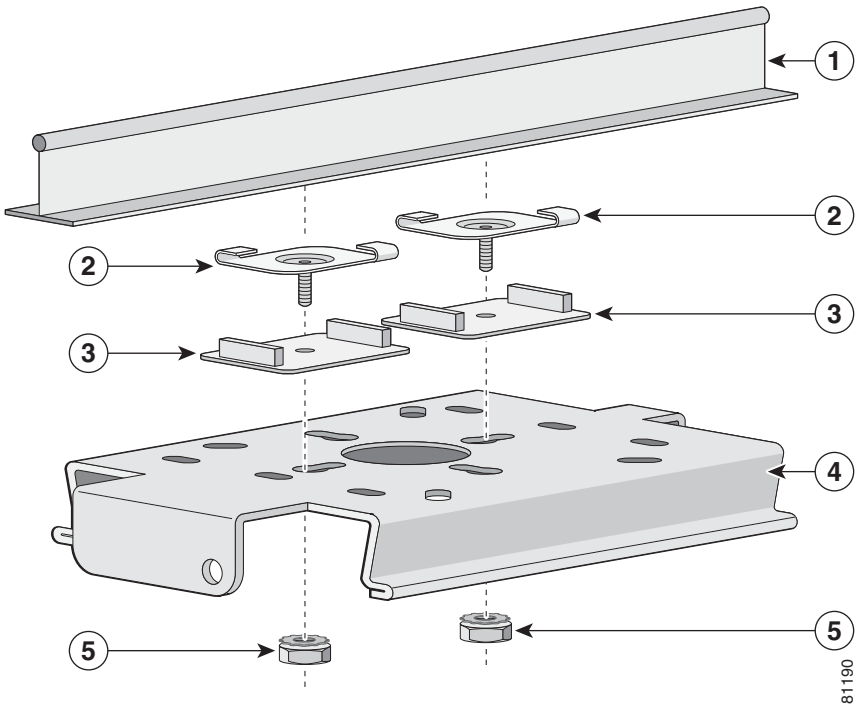
Note On a vertical surface, be sure to mount the bracket with its security hasp facing down.

Step 5 Line up the mounting slots on the access point with the mounting rail on the mounting bracket and slide down the mounting rails until it clicks into place.

Mounting on a Suspended Ceiling

Follow these steps to mount your access point on a suspended ceiling. It may be helpful to refer to Figure 3-2 before beginning the process.

Figure 3-2 Suspended Ceiling Mounting Bracket Parts



1	Suspended ceiling T-rail	**4**	Wall or ceiling mounting bracket
2	Caddy fastener	**5**	Keps nut
3	Plastic spacer		

Step 1 Determine the location at which to mount the access point.

Step 2 Attach two caddy fasteners to the ceiling's T-rail.

Step 3 Use the wall or ceiling mounting bracket to adjust the distance between the caddy fasteners so that they align with the holes in the bracket.

- The distance between the caddy fastener studs is 2.5 in (6.35 cm).

Step 4 Use a standard screwdriver to tighten the caddy fastener studs in place on the T-rail. Do not overtighten.

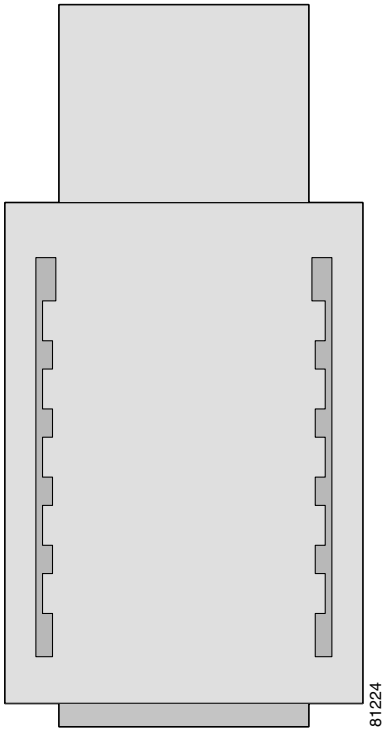
Step 5 Install a plastic spacer on each caddy fastener stud. The spacer's legs should contact the ceiling grid T-rail.

Step 6 Attach the wall or ceiling mounting bracket to the caddy fastener studs and start a Keps nut on each stud.

Step 7 Use a wrench or pliers to tighten the Keps nuts. Do not overtighten.

Step 8 Line up the mounting slots on the access point with the mounting rail on the wall or ceiling mounting bracket and slide it down the mounting rails until it clicks into place. See Figure 3-3.

Figure 3-3 Access Point Mounting Slots

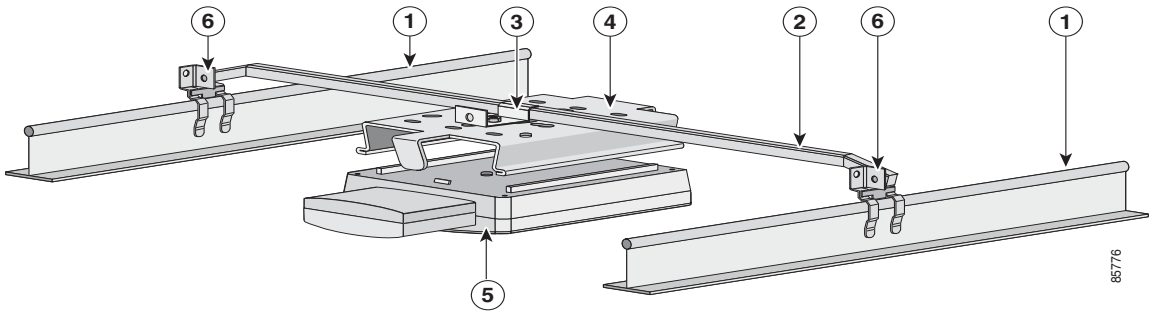


Mounting Above a Suspended Ceiling

The access point mounting bracket is designed to be integrated into the T-bar grid above the tiles of a suspended ceiling. The access point uses a T-bar box hanger (not supplied) such as the Erico Caddy 512 or B-Line BA12 and should be oriented just above the top surface of a standard 5/8-in. (1.59 cm) ceiling tile. You may need to modify a thicker tile to allow room for the access point.

Follow these steps to mount the access point above a suspended ceiling. Refer Figure 3-4 before proceeding.

Figure 3-4 T-Bar Grid Mounting Bracket Parts

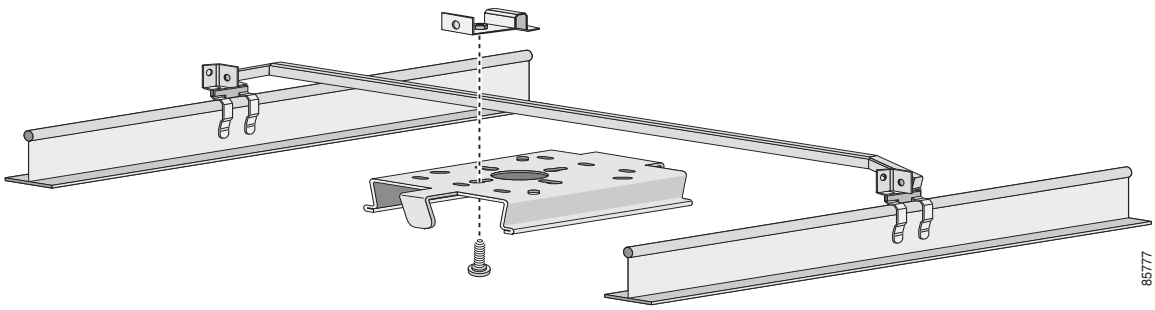


1	Suspended ceiling T-rail	**4**	Access point mounting bracket
2	T-bar box hanger	**5**	Access point
3	Bracket mounting clip	**6**	T-rail clip

Step 1 Insert the bracket mounting clip's tab into the large hole on the access point mounting bracket.

Step 2 Place the clip over the T-bar box hanger (refer to Figure 3-5) and secure it to the access point mounting bracket with the 1/4-20 fastener (supplied with the T-bar hanger).

Figure 3-5 T-Bar and Mounting Bracket



Note Figure 3-5 shows the access point mounting bracket mounted perpendicular to the T-bar box hanger. You can also mount the bracket parallel to the T-bar box hanger.

Step 3 Remove a ceiling tile adjacent to the mounting location.

Step 4 Configure the ends of the T-bar box hanger to allow for maximum clearance above the ceiling tile. See the illustration above.

Step 5 Attach the T-rail clips on the each end of the T-bar box hanger to the ceiling grid T-rails. Make sure the clips are securely attached to the T-rails.

Step 6 Connect a drop wire to a building structural element and the hole provided in the bracket mounting clip. This additional support is required in order to comply with the U.S. National Electrical Safety Code.

Step 7 Attach the access point to the access point mounting bracket.

Step 8 Connect the Ethernet cables to the access point.

Note The power module and power injector are not rated for mounting above suspended ceilings. Therefore, you must use the Ethernet cable to supply power.

Step 9 If you need additional security, you can secure the access point to a nearby immovable object using a Kensington lock and security cable.

Step 10 Verify that the access point is operating before replacing the ceiling tile.

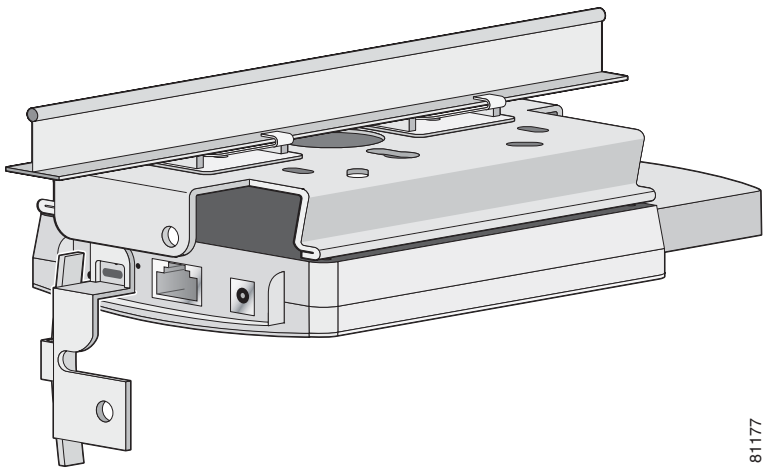
Using the Security Hasp Adapter

The security hasp on the wall or ceiling mounting bracket and the security hasp adapter locks the access point to the bracket to make it more secure. After you have installed the access point on the detachable mounting bracket, follow these steps to secure it with a padlock (Master Lock model 120T, 121T or equivalent).

Step 1 Connect the Ethernet cable and power jack.

Step 2 Insert the T-shaped tab on the security hasp adapter into the Kensington lock slot on the access point. See Figure 3-6.

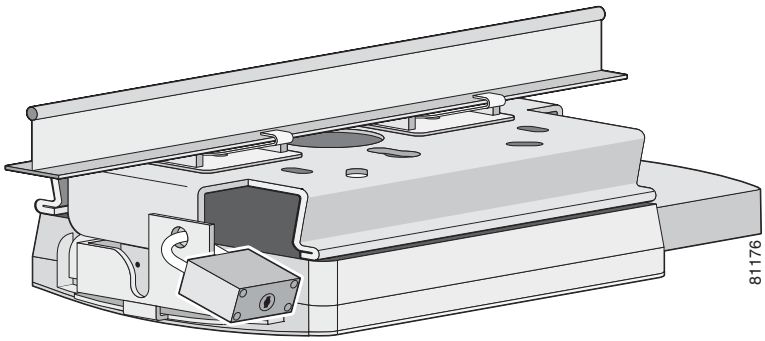
Figure 3-6 Security Hasp Adapter



Step 3 Rotate the adapter to engage it with the security hasp. The hole in the adapter should be aligned with the hole in the security hasp.

Step 4 Secure the adapter to the security hasp with a padlock. Your installation will look similar to Figure 3-7.

Figure 3-7 Security Hasp with Padlock



Mounting on a Cubical Wall Partition

Follow these steps to mount the access point on a cubical wall partition.

Step 1 Select the place on the partition where you want to mount the access point.

Step 2 Determine the width of the partition you are going to mount the access point on.

Step 3 Assemble the cubical partition mounting bracket by sliding the two pieces together. You can use either the short or long part of the bracket to obtain the proper fit to the partition wall.

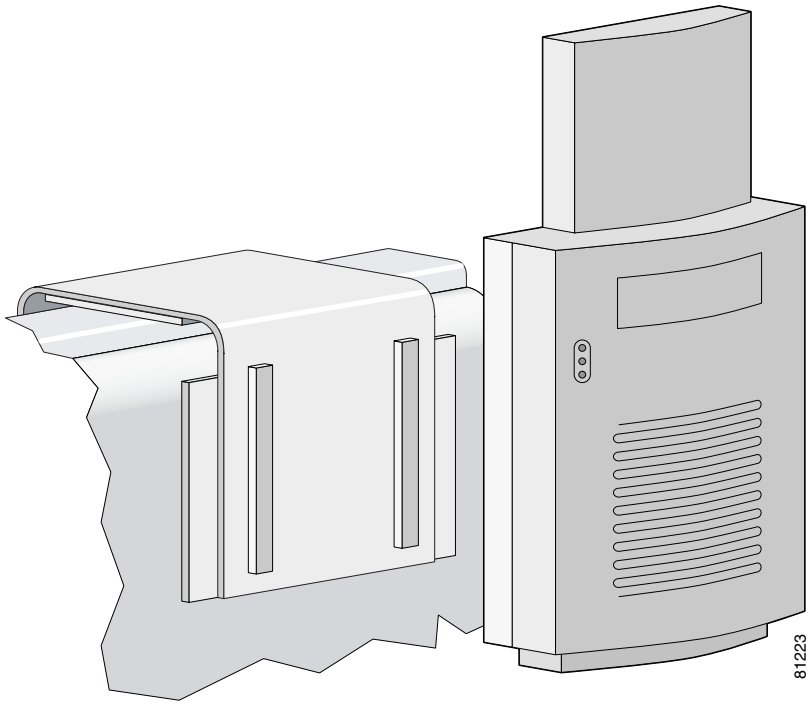
- The bracket is adjustable from 2.125 in. (5.39 cm) to 4.25 in. (10.79 cm).

Step 4 Connect the Ethernet and power cables.

Step 5 Line up the mounting slots on the access point with the mounting rails on the cubical partition mounting bracket and slide it down the rails until it clicks into place.

Step 6 Position the mounting bracket over the partition wall and adjust it to fit. See Figure 3-8.

Figure 3-8 Cubicle Wall Bracket



Using the Desktop Holster

Follow these steps to mount the access point on a desktop or other horizontal surface using the supplied desktop holster.

Step 1 Select a suitable location to place the holster.

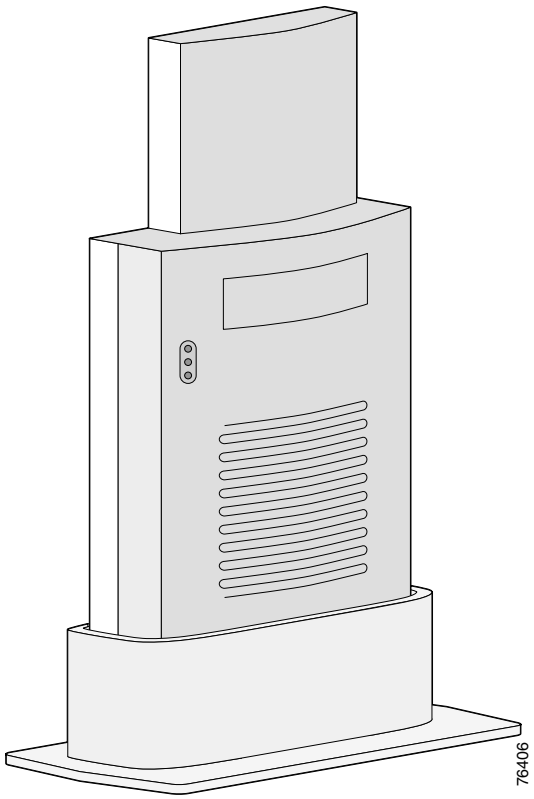
Step 2 Connect the Ethernet and power cables.

- If you are going to secure the access point with a Kensington lock, attach it now.

Step 3 Position the holster so that its back side is facing you.

Step 4 Insert the access point into the holster while guiding the cables so that they do not interfere with the sides of the holster. You will hear a click when the access point locks into place. See Figure 3-9.

Figure 3-9 Desktop Holster



Using the Cable Lock Feature

When you mount the access point using the cubical partition mount or desktop holster, you can secure the access point with your own security cable. Follow these steps to install the security cable.

Note Cisco recommends using a Kensington Notebook Microstar (model number 64068) to secure your access point.

Step 1 Loop the security cable around a nearby immovable object.

Step 2 Insert the key into the lock.

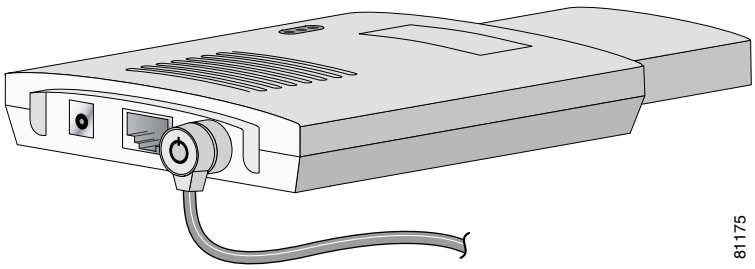
Step 3 Insert the lock into the security slot on the access point.

Step 4 Rotate the key right or left to secure the lock to the access point.

Step 5 Remove the key.

A properly secured lock and cable look similar to Figure 3-10.

Figure 3-10 Kensington Lock



CHAPTER 4

2.4-GHz Radio Upgrade for Autonomous Access Points

This chapter provides upgrade instructions for the autonomous access point 2.4-GHz (IEEE 802.11b-compliant or IEEE 802.11g-compliant) radio card and includes the following sections:

Upgrade Overview

This section provides instructions for upgrading the autonomous access point 2.4-GHz radio.

Caution Your autonomous access point must be running Cisco IOS 12.2(13)JA or later before you upgrade to the IEEE 802.11g-compatible radio, otherwise your access point may not be able to complete the boot sequence until the radio is removed. For additional information, refer to the "Finding the Software Version" section.

The following operations summarize the upgrade procedure:

1. Remove all cables and power connections from the access point.
2. Follow standard electrostatic discharge (ESD) procedures.
3. Place the access point on an ESD-protected work surface.
4. Remove the access point's back cover.
5. Remove the existing 2.4-GHz radio card.
6. Install the new 2.4-GHz radio card.
7. Replace the access point's back cover.
8. Install the new compliance label.

Caution ESD can damage the Cisco Aironet radio and the internal components of the access point. It is recommended that the 2.4-GHz radio upgrade procedures be performed by an ESD-trained service technician at an ESD-protected workstation.

Note After you install the new radio, all configurable radio settings will be at default values. Refer to the Cisco IOS Software Configuration Guide for Cisco Aironet Access Pointsfor complete instructions on configuring the new radio.

Unpacking the Radio

Each 2.4-GHz (IEEE 802.11g) radio is shipped with the following items:

- Quick Start Guide
- A product registration card
- A 1100 series access point product compliance label
- A 1200 series access point product compliance label (not used on 1100 series access points)
- A 1200 series access point 2.4-GHz radio compliance label (not used on 1100 series access points)
- A T-10 tamper-resistant Torx L-wrench (not used on 1100 series access points)

If anything is missing or damaged, contact your Cisco representative for support.

Removing the Back Cover

To remove the access point's back cover, follow these steps:

Step 1 Remove all cables and power connections from the access point.

Step 2 Remove all static-generating items from the work area, such as plastic material, styrofoam cups, and other similar items.

Step 3 Place the access point and the new 2.4-GHz radio (in its antistatic bag) on an antistatic work surface.

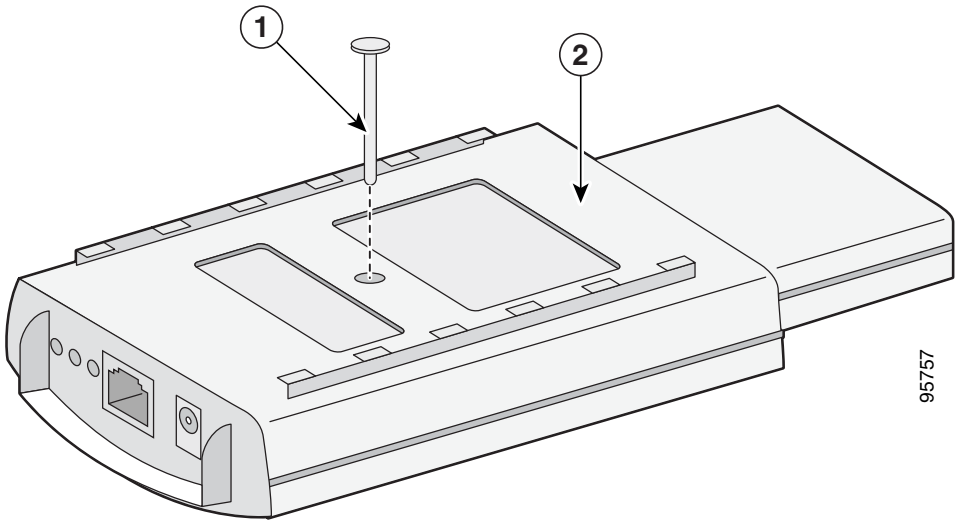
Step 4 Discharge any static buildup on your body by touching a grounded surface (antistatic work surface) before proceeding.

Step 5 Position the access point so that the back cover is facing up.

Caution The internal access point components and the 2.4-GHz radio can be damaged by ESD from improper handling.

Step 6 Remove the back-cover retaining screw using a Philips screwdriver (see Figure 4-1).

Figure 4-1 Access Point Back Cover Screw



1	Back cover screw	**2**	Back cover

Step 7 Hold the front cover with one hand, and with the other hand gently slide the back cover towards the connector end of the unit.

Step 8 Gently lift the connector end of the back cover and remove the cover.

Go to the "Removing a 2.4-GHz Radio" section.

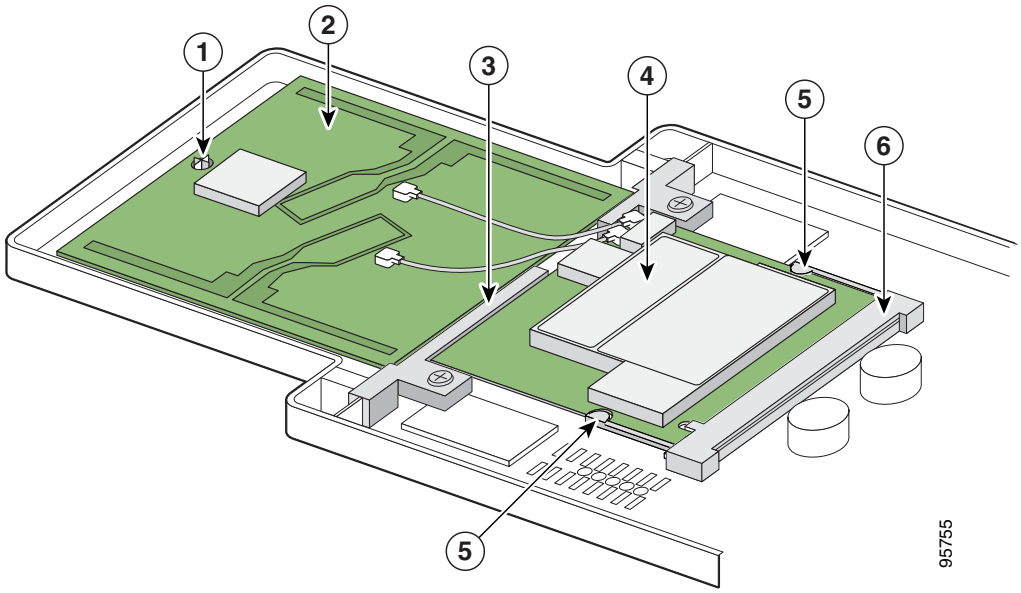
Removing a 2.4-GHz Radio

To remove a 2.4-GHz radio card from your access point, follow these steps:

Caution The internal access point components and the 2.4-GHz radio can be damaged by ESD from improper handling.

Step 1 Gently lift the top of the antenna card until it clears the plus shaped (+) support post (see Figure 4-2).

Figure 4-2 Radio Card and Antenna Card



1	Support post	**4**	Radio Card
2	Antenna card	**5**	Card-retaining clips
3	Support bracket	**6**	Mini-PCI connector

Step 2 Gently pull the antenna card to remove it from the notch in the support bracket. Do not disconnect the antenna wire connectors.

Step 3 Push the card-retaining clips (on each side of card) away from the radio card (see Figure 4-2). When released, the radio card springs up. Do not disconnect the antenna wires.

Note If the radio card does not spring up, slightly loosen the support bracket screws.

Step 4 Remove the 2.4-GHz radio card from the mini-PCI connector:

a. Grasp the radio card only on the edges, being careful not to touch components on the board or the gold connector pins.

b. Remove the 2.4-GHz card from the mini-PCI connector.

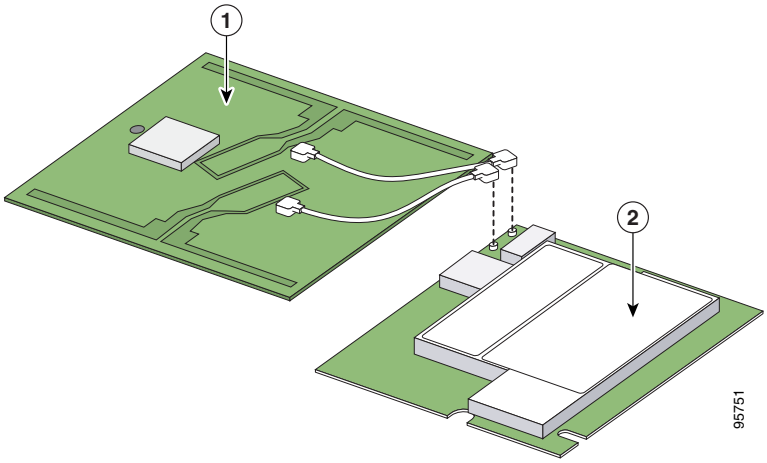
Step 5 Place the radio card and antenna card on the ESD-protected work surface.

Step 6 Use your fingernail to carefully remove the antenna wire connectors from the 2.4-GHz radio card. Do not remove the antenna wire connectors from the antenna board.

Caution The antenna connectors can be damaged if you use long-nose pliers during the removal process.

Caution To avoid damaging the antenna wire assemblies, handle them by their connectors.

Figure 4-3 Antenna Wires



1	Antenna card	**2**	Radio card

Step 7 Place the removed 2.4-GHz radio card into an anti-static bag. The antenna card connects to your new radio card.

Go to the "Installing a 2.4-GHz Radio" section.

Installing a 2.4-GHz Radio

To install a new 2.4-GHz radio card into the access point, follow these steps:

Caution The internal access point components and the 2.4-GHz radio can be damaged by ESD from improper handling.

Step 1 Carefully remove the new Cisco Aironet 2.4-GHz radio card from its anti-static bag.

Step 2 Grasp the radio card only on the edges, being careful not to touch components on the board or the gold connector pins.

Step 3 Place the radio card on the anti-static work surface next to the antenna card.

Step 4 Use your fingers to carefully connect the antenna wire connectors to the connectors on the 2.4-GHz radio card (see Figure 4-3).

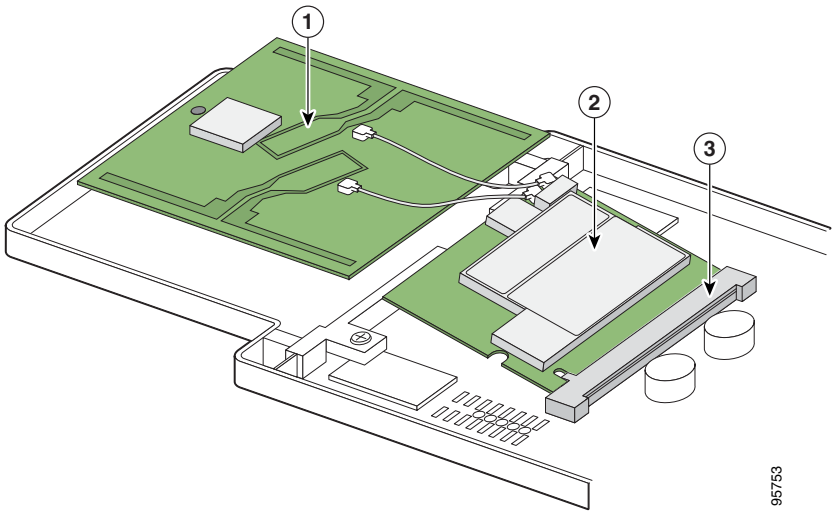
Caution The antenna connectors can be damaged by using a pair of long-nose pliers.

Caution To avoid damaging the antenna wire assemblies, handle them by their connectors.

Step 5 Insert the radio card into the access point's mini-PCI connector by following these steps:

a. Tilt the radio card at approximately 20° to 30° so that its gold pins are aligned with the mini-PCI connector (see Figure 4-4).

Figure 4-4 Inserting Radio Card in Mini-PCI Connector



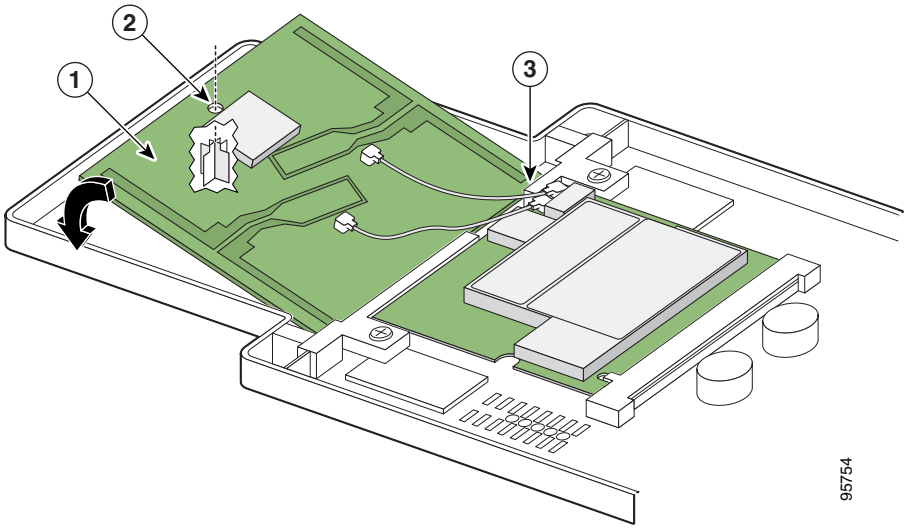
1	Antenna card	**3**	Mini-PCI connector
2	Radio card		

b. Push the radio card into the mini-PCI connector until it is fully seated (you will hear a slight snap).

Step 6 Hold the top of the antenna card with one hand and carefully push the radio card down with your other hand (towards the access point's motherboard) until the card-retaining clips lock into the notches on the side of the radio card (you will hear a click).

Step 7 Insert the antenna card into the notch in the support bracket and gently push until it is seated (see Figure 4-5).

Figure 4-5 Inserting Antenna Card



1	Antenna card	**3**	Support bracket notch
2	Support post hole		

Step 8 Align the hole on the top of the antenna board with the support post and gently push down until the board is fully seated on the support post (see Figure 4-5).

Step 9 Verify the following:

a. The radio car is properly secured with both retaining clips engaged.

b. The antenna board is properly seated.

c. The antenna connectors are not touching.

Caution Do not allow antenna connectors to touch while power is applied, or the radio can be damaged. If they are touching, carefully rotate them in opposite directions until they are separated.

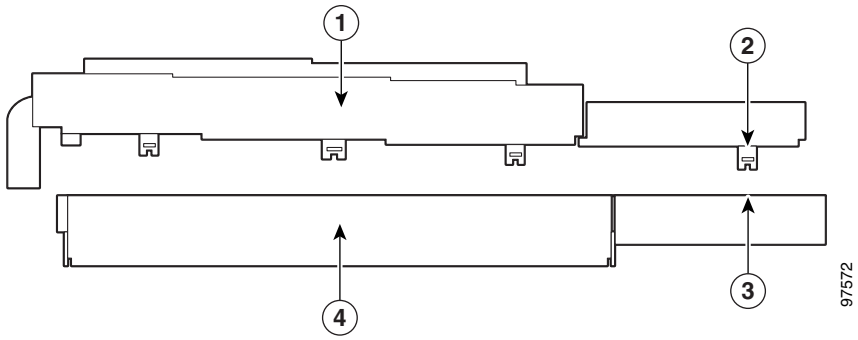
Go to the "Replacing the Back Cover" section on page 4-8.

Replacing the Back Cover

To replace the back cover on the access point, follow these steps:

Step 1 While holding the back cover near the connector end of the access point, position it at a slight angle and carefully place the latches on the antenna end into the detents on the antenna end of the front cover (refer to Figure 4-6).

Figure 4-6 Positioning the Back Cover Latches



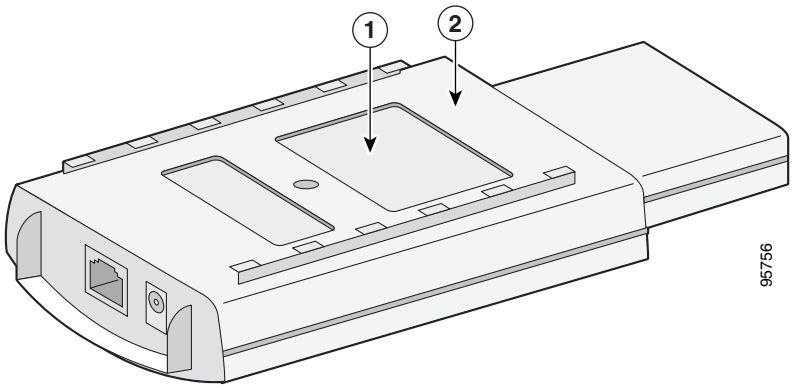
1	Back cover	**3**	Antenna end detent
2	Antenna end latch	**4**	Front cover

Step 2 Release the back cover and with one finger gently push the connector end of the back cover towards the antenna end. The back cover drops into place and slides forward until it is fully seated.

Step 3 Use a Philips screwdriver to hand tighten the cover's retaining screw.

Step 4 Remove the backing paper from the 1100 series access point product compliance label and carefully place the new label over the existing label (see Figure 4-7).

Figure 4-7 Location of Compliance Labels



1	Product compliance label	**2**	Back cover

The radio card installation is now complete. To configure the new radio with your new wireless network settings, refer to the Cisco IOS Software Configuration Guide for Cisco Aironet Access Points.

Finding the Software Version

To find the version of operating system software running on your autonomous access point, refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points.*

Troubleshooting Autonomous Access Points

This chapter provides troubleshooting procedures for basic problems with the 1100 series autonomous access point. For the most up-to-date, detailed troubleshooting information, refer to the Cisco Technical Support and Documentation website at the following URL:

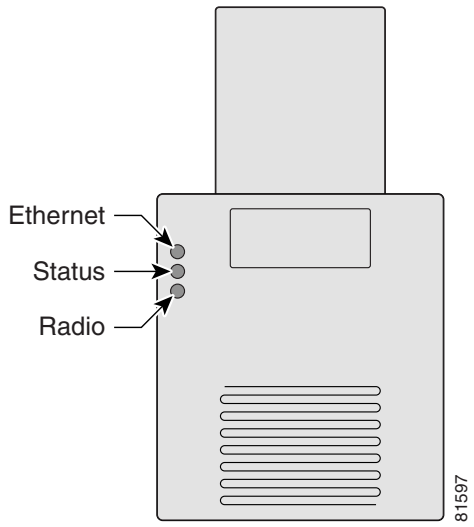
http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

Sections in this chapter include:

Checking the Autonomous Access Point LEDs

If your autonomous access point is not communicating, check the three LEDs on the top panel. You can use them to quickly assess the unit's status. Figure 5-1 shows the LEDs.

Figure 5-1 Access Points



The LEDs signals have the following meanings (for additional details refer to Table 5-1):

- The Ethernet LED signals traffic on the wired LAN, or Ethernet infrastructure. This LED is normally green when an Ethernet cable is connected, and blinks green when a packet is received or transmitted over the Ethernet infrastructure. The LED is off when the Ethernet cable is not connected.
- The status LED signals operational status. Steady green indicates that the access point is associated with at least one wireless client. Blinking green indicates that the access point is operating normally but is not associated with any wireless devices.
- The radio LED blinks green to indicate radio traffic activity. The light is normally off, but it blinks green whenever a packet is received or transmitted over the access point's radio.

Table 5-1 Top Panel LED Signals

Message type	Ethernet LED	Status LED	Radio LED	Meaning
Boot loader status	Green	–	Green	DRAM memory test.
	–	Amber	Red	Board initialization test
	–	Blinking green	Blinking green	Flash memory test.
	Amber	Green	–	Ethernet initialization test.
	Green	Green	Green	Starting Cisco IOS.
Association status	–	Green	–	At least one wireless client device is associated with the unit.
	–	Blinking green	–	No client devices are associated; check the unit's SSID and WEP settings.
Operating status	–	Green	Blinking green	Transmitting/receiving radio packets.
	Green	–	–	Ethernet link is operational.
	Blinking green	–	–	Transmitting/receiving Ethernet packets.
Boot Loader Errors	Red	–	Red	DRAM memory test failure.
	–	Red	Red	File system failure.
	Red	Red	–	Ethernet failure during image recovery.
	Amber	Green	Amber	Boot environment error.
	Red	Green	Red	No Cisco IOS image file.
	Amber	Amber	Amber	Boot failure.
Operation Errors	–	Green	Blinking amber	Maximum retries or buffer full occurred on the radio.
	Blinking amber	–	–	Transmit/receive Ethernet errors.
	–	Blinking amber	–	General warning.
Configuration Reset	–	Amber	–	Resetting the configuration options to factory defaults.
Failure	Red	Red	Red	Firmware failure; try disconnecting and reconnecting unit power.
Firmware Upgrade	–	Red	–	Loading new firmware image.

Checking Basic Settings

Mismatched basic settings are the most common causes of lost connectivity with wireless clients. If the access point does not communicate with client devices, check the following areas.

Default IP Address Behavior

When you connect an 1100 series access point running Cisco IOS Release 12.3(2)JA or later with a default configuration to your LAN, the 1100 series access point makes several attempts to get an IP address from the DHCP server. If it does not receive an address, it assigns itself the IP address 10.0.0.1 for five minutes and does not become a mini-DHCP server. During this five-minute window, you can browse to the default IP address and configure a static address. If after five minutes the access point is not reconfigured, it discards the 10.0.0.1 address and reverts to requesting an address from the DHCP server. If it does not receive an address, it sends requests indefinitely. If you miss the five-minute window for browsing to the access point at 10.0.0.1, you can power-cycle the access point to repeat the process.

When you connect an 1100 series access point running Cisco IOS Release 12.2(15)JA or earlier with a default configuration to your LAN, the 1100 series access point makes several attempts to get an IP address from the DHCP server. If it does not receive an address, it assigns itself the IP address 10.0.0.1 and becomes a mini-DHCP server. In that capacity, the access point provides up to twenty IP addresses between 10.0.0.11 and 10.0.0.30 to the following devices:

- An Ethernet-capable PC connected to its Ethernet port
- Wireless client devices configured to use either no SSID or tsunami as the SSID, and with all security settings disabled

The mini-DHCP server feature is disabled automatically when you assign a static IP address to the access point.

Caution When the access point is connected to your LAN, the access point mini-DHCP server provides an IP address to any DHCP requests it receives.

Default SSID and Radio Behavior

In Cisco IOS Relese 12.3(2)JA2 and earlier, the access point radio is enabled by default and the default SSID is *tsunami*.

In Cisco IOS Release 12.3(4)JA and later, the access point radio is disabled by default, and there is no default SSID. You must create an SSID and enable the radio before the access point will allow wireless associations from other devices. These changes to the default configuration improve the security of newly installed access points. Refer to the *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for instructions on configuring the SSID and the "Enabling the Radio Interfaces" section on page 5-5 for instructions on enabling the radio interface.

Enabling the Radio Interfaces

To enable the radio interface, follow these instructions:

Step 1 Open your web browser and enter the access point's IP address in the browser address line. Press **Enter**. An Enter Network Password window appears.

Step 2 Enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.

Step 3 When the Summary Status page displays, click **Network Interfaces > Radio0-802.11B** or **Radio0-802.11G** and the radio status page displays.

Step 4 Click **Settings** and the radio settings page displays.

Step 5 Click **Enable** in the Enable Radio field.

Step 6 Click **Apply**.

SSID

Wireless clients attempting to associate with the access point must use the same SSID as the access point. If a client device's SSID does not match the SSID of an access point in radio range, the client device will not associate. The access point default SSID is *tsunami*.

Note In Cisco IOS Release 12.3(4)JA, there is no default SSID. You must configure an SSID before client devices can associate to the access point.

WEP Keys

The WEP key you use to transmit data must be set up exactly the same on your access point and any wireless devices with which it associates. For example, if you set WEP Key 3 on your client adapter to 0987654321 and select it as the transmit key, you must also set WEP Key 3 on the access point to exactly the same value. The access point does not need to use Key 3 as its transmit key, however.

Refer to *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points* for instructions on setting the access point's WEP keys.

Security Settings

Wireless clients attempting to authenticate with your access point must support the same security options configured in the access point, such as EAP or LEAP, MAC address authentication, Message Integrity Check (MIC), WEP key hashing, and 802.1X protocol versions.

If a wireless client is unable to authenticate with your access point, contact the system administrator for proper security settings in the client adapter and for the client adapter driver and firmware versions that are compatible with the access point settings.

Note The access point MAC address that appears on the Status page in the Aironet Client Utility (ACU) is the MAC address for the access point radio. The MAC address for the access point Ethernet port is printed on the label on the back of the access point.

Running the Carrier Busy Test

You can use the carrier busy test to find the least congested channel for the radio interface (802.11b). You should typically run the test several times to obtain the best results and to avoid temporary activity spikes.

Note The carrier busy test is primarily used for a single access point or a bridge environment. For sites with multiple access points, a site survey is typically performed to determine the best operating locations and operating frequencies for the access points.

Note All associated clients on the selected radio will be disassociated during the 6 to 8 seconds needed for the carrier busy test.

Follow these steps to activate the carrier busy test:

Step 1 Open your web browser and enter the access point's IP address in the browser address line. Press **Enter**. An Enter Network Password window appears.

Step 2 Enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.

Step 3 Click **Network Interfaces** and the Network Interface Summary page displays.

Step 4 Choose the radio interface experiencing problems by clicking **Radio0-802.11B**. The radio status page displays.

Step 5 Click the **Carrier Busy Test** tab and the Carrier Busy Test page displays.

Step 6 Click **Start** to begin the carrier busy test.

When the test completes, the results are displayed on the bottom of the page. For each of the channel center frequencies, the test produces a value indicating the percentage of time that the channel is busy.

Running the Ping or Link Test

You can use the ping or link test to evaluate the communication link with an associated access point. With the ping or link test you can:

a. Perform a test using a specified number of packets and then display the test results.

b. Perform a test that continuously operates until you stop it and then display the test results.

Follow these steps to activate the ping or link test:

Step 1 Open your web browser and enter the access point's IP address in the browser address line. Press **Enter**. An Enter Network Password window appears.

Step 2 Enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.

Step 3 Click **Association** and the main association page displays.

Step 4 Click the MAC address of an associated access point, and the Statistics page for that device displays.

Step 5 Click the **Ping/Link Test** tab and the Ping/Link Test page displays.

Step 6 If you want to specify the number of packets to use in the test, follow these steps:

a. Enter a number of packets in the Number of Packets field

b. Enter a packet size (1 to 1400 bytes) in the Packet Size field.

c. Click **Start**. The test automatically stops when all packets are utilized.

Step 7 If you want to use a continuous test, follow these steps:

a. Enter a packet size in the Packet Size field.

b. Click **Start** to activate the test.

c. Click **Stop** to stop the test.

When the test stops, the test results are displayed at the bottom of the page. You should check for lost packets that might indicate a problem with the wireless link. For best results, you should perform this test several times.

Resetting to the Default Configuration

If you forget the password that allows you to configure the access point, you may need to completely reset the configuration. You can use the MODE button on the access point or the web-browser interface.

Note The following steps reset *all* configuration settings to factory defaults, including passwords, WEP keys, the IP address, and the SSID.

For additional information on access point default behavior, refer to the "Default IP Address Behavior" section on page 5-4 and the "Default SSID and Radio Behavior" section on page 5-4.

Using the MODE Button

Follow these steps to delete the current configuration and return all access point settings to the factory defaults using the MODE button:

Step 1 Disconnect power (the power jack for external power or the Ethernet cable for in-line power) from the access point.

Step 2 Press and hold the MODE button while you reconnect power to the access point.

Step 3 Hold the MODE button until the Status LED turns amber (approximately 2 to 3 seconds), and release the button.

Step 4 After the access point reboots, you must reconfigure the access point by using the Web browser interface, the Telnet interface, or Cisco IOS commands.

Note The access point is configured with the factory default values including the IP address (set to receive an IP address using DHCP).

Using the Web Browser Interface

Follow the steps below to delete the current configuration and return all access point settings to the factory defaults using the web browser interface.

Step 1 Open your web browser and enter the access point's IP address in the browser address line. Press **Enter**. An Enter Network Password window appears.

Step 2 Enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive. The Summary Status page appears.

Step 3 Click **System Software** and the System Software screen appears.

Step 4 Click **System Configuration** and the System Configuration screen appears.

Step 5 Click **Default**.

Note If the access point is configured with a static IP address, the IP address does not change.

Step 6 After the access point reboots, you must reconfigure the access point by using the Web browser interface, the Telnet interface, or Cisco IOS commands.

Reloading the Access Point Image

If your access point has a firmware failure, you must reload the complete access point image file using the Web browser interface or by pressing and holding the MODE button for about 20 to 30 seconds. You can use the browser interface if the access point firmware is still fully operational and you want to upgrade the firmware image. However, you can use the MODE button when the access point has a corrupt firmware image.

Using the MODE button

You can use the MODE button on the access point to reload the access point image file from an active Trivial File Transfer Protocol (TFTP) server on your network or on a PC connected to the access point Ethernet port.

Note If your access point experiences a firmware failure or a corrupt firmware image, indicated by three red LEDs, you must reload the image from a connected TFTP server.

Note This process resets *all* configuration settings to factory defaults, including passwords, WEP keys, the access point IP address, and SSIDs.

Follow these steps to reload the access point image file:

Step 1 The PC you intend to use must be configured with a static IP address in the same subnet as the access point.

Step 2 Place a copy of the desired access point image file (such as c1100-k9w7-tar.123-8.JA.tar) into the TFTP server folder on your PC. For additional information, refer to the "Obtaining the Access Point Image File" and "Obtaining the TFTP Server Software" sections.

Step 3 Rename the access point image file in the TFTP server folder to **c1100-k9w7-tar.default**.

Step 4 Activate the TFTP server.

Step 5 Connect the PC to the access point using a Category 5 (CAT5) Ethernet cable.

Step 6 Disconnect power (the power jack for external power or the Ethernet cable for in-line power) from the access point.

Step 7 Press and hold the MODE button while you reconnect power to the access point.

Step 8 Hold the MODE button until the status LED turns red (approximately 20 to 30 seconds), and release the MODE button.

Step 9 Wait until the access point reboots as indicated by all LEDs turning green followed by the Status LED blinking green.

Step 10 After the access point reboots, you must reconfigure the access point by using the Web interface, the Telnet interface, or Cisco IOS commands.

Web Browser Interface

You can also use the Web browser interface to reload the access point image file. The Web browser interface supports loading the image file using HTTP or TFTP interfaces.

Note Your access point configuration is not changed when using the browser to reload the image file.

Browser HTTP Interface

The HTTP interface enables you to browse to the access point image file on your PC and download the image to the access point. Follow these instructions to use the HTTP interface:

Step 1 Open your web browser and enter the access point's IP address in the browser address line. Press **Enter**. An Enter Network Password window appears.

Step 2 Enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive.

Step 3 The Summary Status page appears.

Step 4 Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.

Step 5 Click the **Browse** button to locate the access point image file (such as c1100-k9w7-tar.123-8.JA.tar) on your PC.

Step 6 Click **Upload**.

Step 7 When a message appears that indicates the upgrade is complete, click **OK**.

For additional information, click the **Help** icon on the Software Upgrade screen.

Browser TFTP Interface

The TFTP interface allows you to use a TFTP server on a network device to load the access point image file. Follow these instructions to use a TFTP server:

Step 1 Open your web browser and enter the access point's IP address in the browser address line. Press **Enter**. An Enter Network Password window appears.

Step 2 Enter the administrator username and password. The default username is *Cisco* and the default password is *Cisco*. The username and password are case sensitive. The Summary Status page appears.

Step 3 Click the **System Software** tab and then click **Software Upgrade**. The HTTP Upgrade screen appears.

Step 4 Click the **TFTP Upgrade** tab.

Step 5 Enter the IP address for the TFTP server in the TFTP Server field.

Step 6 Enter the file name for the access point image file (such as c1100-k9w7-tar.123-7.JA.tar) in the Upload New System Image Tar File field. If the file is located in a subdirectory of the TFTP server root directory, include the relative path of the TFTP server root directory with the filename. If the file is located in the TFTP root directory, enter only the filename.

Step 7 Click **Upload**.

Step 8 When a message appears that indicates the upgrade is complete, click **OK**.

For additional information click the Help icon on the Software Upgrade screen.

Obtaining the Access Point Image File

The access point image file can be obtained from the Cisco.com software center using the following steps:

Step 1 Use your Internet browser to access the Cisco Software Center at the following URL:

http://www.cisco.com/cisco/software/navigator.html

Step 2 Click **Wireless LAN Access > Aironet Access Points > Cisco Aironet 1100 Series**.

Step 3 Click **Cisco Aironet 1100 Access Point**.

Step 4 On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.

Step 5 Click **IOS**.

Step 6 Choose the Cisco IOS release desired, such as 12.3.11.JA.

Step 7 Click **WIRELESS LAN** for an access point image file, such as c1100-k9w7-tar.123-11.JA.tar.

Step 8 On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.

Step 9 On the Security Information window, click **Yes** to display non-secure items.

Step 10 On the Encryption Software Export Authorization page, read the information and check **Yes** or **No** to the question asking if the image is for use by you or your organization. Click **Submit**.

Step 11 If you checked No, enter the requested information and click **Submit**.

Step 12 Click **Yes** to continue.

Step 13 Click **DOWNLOAD**.

Step 14 Read and accept the terms and conditions of the Software Download Rules.

Step 15 On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.

Step 16 Click **Save** to download your image file to your hard disk.

Step 17 Select the desired download location on your hard disk and click **Save**.

Obtaining the TFTP Server Software

You can download TFTP server software from several websites. Cisco recommends the shareware TFTP utility available at this URL:

http://tftpd32.jounin.net

Follow the instructions on the website for installing and using the utility.

CHAPTER 6

Troubleshooting Lightweight Access Points

This chapter provides troubleshooting procedures for basic problems with the 1100 series lightweight access point. For the most up-to-date, detailed troubleshooting information, refer to the Cisco Technical Support and Documentation website at the following URL:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

Sections in this chapter include:

Guidelines for Using 1100 Series Lightweight Access Points

Keep these guidelines in mind when you use a 1100 series lightweight access point:

- The access points can only communicate with Cisco 2006 or 4400 series wireless LAN controllers.

Note Cisco 4100 series, Airespace 4012 series, and Airespace 4024 series wireless LAN controllers are not supported because they lack the memory required to support access points running Cisco IOS software.

- The access points do not support Wireless Domain Services (WDS) and cannot communicate with WDS devices. However, the controller provides functionality equivalent to WDS when the access point associates to it.
- The access points support eight Basic Service Set Identifiers (BSSIDs) per radio and a total of eight wireless LANs per access point. When the access point associates to a controller, only wireless LANs with IDs 1 through 8 are pushed to the access point.
- The access points do not support Layer 2 LWAPP. They must get an IP address and discover the controller using DHCP, DNS, or IP subnet broadcast.
- The access points do not have a console port.

Note You are unable to manually configure controller information on the 1100 series lightweight access point, because it does not have a console port.

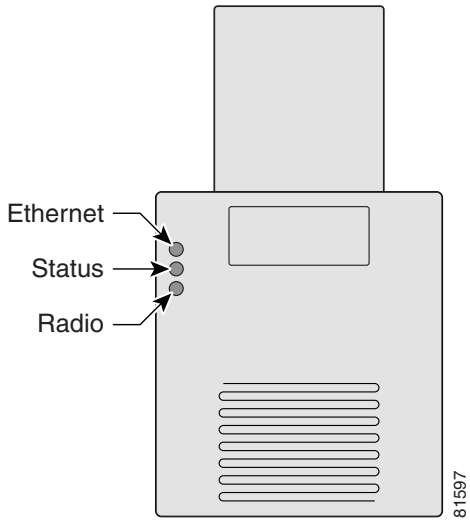
Using DHCP Option 43

You can use DHCP Option 43 to provide a list of controller IP addresses to the access points, enabling the access point to find and join a controller. For additional information, refer to the "Configuring DHCP Option 43 for Lightweight Access Points" section on page F-1.

Checking the Lightweight Access Point LEDs

If your access point is not communicating, check the three LEDs on the top panel. You can use them to quickly assess the unit's status. Figure 6-1 shows the LEDs.

Figure 6-1 Access Points LEDs



The LEDs signals have the following meanings (for additional details refer to Table 6-1):

- The Ethernet LED signals traffic on the wired LAN, or Ethernet infrastructure. This LED is normally green when an Ethernet cable is connected, and blinks green when a packet is received or transmitted over the Ethernet infrastructure. The LED is off when the Ethernet cable is not connected.
- The status LED signals operational status. Steady green indicates that the access point is associated with at least one wireless client. Blinking green indicates that the access point is operating normally but is not associated with any wireless devices.
- The radio LED blinks green to indicate radio traffic activity. The light is normally off, but it blinks green whenever a packet is received or transmitted over the access point's radio.

Table 6-1 Top Panel LED Signals

Message type	Ethernet LED	Status LED	Radio LED	Meaning
Boot loader status	Green	–	Green	DRAM memory test.
	–	Amber	Red	Board initialization test
	–	Blinking green	Blinking green	Flash memory test.
	Amber	Green	–	Ethernet initialization test.
	Green	Green	Green	Starting Cisco IOS.
Association status	–	Green	–	At least one wireless client device is associated with the unit.
	–	Blinking green	–	No client devices are associated; check the unit's SSID and WEP settings.
Operating status	–	Green	Blinking green	Transmitting/receiving radio packets.
	Green	–	–	Ethernet link is operational.
	Blinking green	–	–	Transmitting/receiving Ethernet packets.
Boot Loader Errors	Red	–	Red	DRAM memory test failure.
	–	Red	Red	File system failure.
	Red	Red	–	Ethernet failure during image recovery.
	Amber	Green	Amber	Boot environment error.
	Red	Green	Red	No Cisco IOS image file.
	Amber	Amber	Amber	Boot failure.
Operation Errors	–	Green	Blinking amber	Maximum retries or buffer full occurred on the radio.
	Blinking amber	-	–	Transmit/receive Ethernet errors.
	–	Blinking amber	–	General warning.
Configuration Reset	–	Amber	–	Resetting the configuration options to factory defaults.
Failure	Red	Red	Red	Firmware failure; try disconnecting and reconnecting unit power.
Firmware Upgrade	–	Red	–	Loading new firmware image.
Controller status	Alternating green, red , and amber[1]			Connecting to the controller. **Note** If the access point remains in this mode for more than five minutes, the access point is unable to find the controller. Ensure a DHCP server is available or that the access point has been primed with the controller information.

1. This status indication has the highest priority and overrides other status indications.

Returning the Access Point to Autonomous Mode

You can return a lightweight access point to autonomous mode by loading a Cisco IOS release that supports autonomous mode (such as Cisco IOS Release 12.3(8)JA or earlier). If the access point is associated to a controller, you can use the controller to load the Cisco IOS release. If the access point is not associated to a controller, you can load the Cisco IOS release using TFTP.

Using a Controller to Return the Access Point to Autonomous Mode

Follow these steps to return a lightweight access point to autonomous mode using a controller:

Step 1 Log into the CLI on the controller to which the access point is associated and enter this command:

config ap tftp-downgrade *tftp-server-ip-address filename access-point-name*
(where:
a) *tftp-server-ip-address* is the IP address of the TFTP server
b) *filename* is the full path and filename of the access point image file, such as D:/Images/*c1100-k9w7-tar.123-8.JA.tar*
c) *access-point-name* is the name that identifies the access point on the ocntroller.)

Step 2 Wait until the access point completes the reboot, as indicated by the Status LED turning green to indicate a client is associated or blinking green to indicate a client is not associated.

Step 3 After the access point reboots, reconfigure it using the access point GUI or the CLI. For additional information refer to the *Cisco Aironet 1100 Series Access Point Hardware Installation Guide* available at this URL:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

To browse to the 1100 series access point documentation, click **Cisco Aironet 1100 Series** listed under "Wireless LAN Access."

Using the MODE Button to Return the Access Point to Autonomous Mode

Follow these steps to return a lightweight access point to autonomous mode using the access point MODE button and a TFTP server:

Note The access point MODE button is enabled by default, but you need to verify that the MODE button is enabled (see the "MODE Button Setting" section on page 6-6).

Step 1 Set the static IP address of the PC on which your TFTP server software runs to an address between 10.0.0.2 and 10.0.0.30.

Step 2 Make sure that the PC contains the access point image file (such as *c1100-k9w7-tar.123-8.JA.tar* for a 1100 series access point) in the TFTP server folder and that the TFTP server is activated.

Step 3 Rename the access point image file in the TFTP server folder to **c1100-k9w7-tar.default.**

Step 4 Connect the PC to the access point using a Category 5 (CAT5) Ethernet cable.

Step 5 Disconnect power from the access point.

Step 6 Press and hold the **MODE** button while you reconnect power to the access point.

Step 7 Hold the **MODE** button until the Radio LED turns red (approximately 20 to 30 seconds) and then release.

Step 8 Wait until the access point reboots, as indicated by all LEDs turning green followed by the Status LED blinking green.

Step 9 After the access point reboots, reconfigure it using the access point GUI or the CLI. For additional information refer to the *Cisco Aironet 1100 Series Access Point Hardware Installation Guide* available at this URL:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

To browse to the 1100 series access point documentation, click **Cisco Aironet 1100 Series** listed under "Wireless LAN Access."

MODE Button Setting

The lightweight access point MODE button is configured from your controller. Use these controller CLI commands to view and configure the MODE button:

```
1) config ap rst-button enable <access-point-name>/all
2) config ap rst-button disable <access-point-name>/all
3) show ap config general <access-point-name>
    (Where access-point-name is the name that identifies the access point on the
    ocntroller.)
```

Obtaining the Autonomous Access Point Image File

The autonomous access point image file can be obtained from the Cisco.com software center using these steps:

Note To download software from the Cisco.com software center, you must be a registered user. You can register from the main Cisco.com web page at this URL: http://cisco.com.

Step 1 Use your Internet browser to access the Cisco Software Center at the following URL:

http://www.cisco.com/cisco/software/navigator.html

Step 2 Click **Wireless LAN Access > Aironet Access Points > Cisco Aironet 1100 Series**.

Step 3 Click **Cisco Aironet 1100 Access Point**.

Step 4 On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.

Step 5 Click **IOS**.

Step 6 Choose the Cisco IOS release desired, such as 12.3.11.JA.

Step 7 Click **WIRELESS LAN** for an access point image file, such as c1100-k9w7-tar.123-11.JA.tar.

Step 8 On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.

Step 9 On the Security Information window, click **Yes** to display non-secure items.

Step 10 On the Encryption Software Export Authorization page, read the information and check **Yes** or **No** to the question asking if the image is for use by you or your organization. Click **Submit**.

Step 11 If you checked No, enter the requested information and click **Submit**.

Step 12 Click **Yes** to continue.

Step 13 Click **DOWNLOAD**.

Step 14 Read and accept the terms and conditions of the Software Download Rules.

Step 15 On the Enter Network Password window, enter your Cisco.com username and password and click **OK**.

Step 16 Click **Save** to download your image file to your hard disk.

Step 17 Select the desired download location on your hard disk and click **Save**.

Obtaining the TFTP Server Software

You can download TFTP server software from several web sites. Cisco recommends the shareware TFTP utility available at this URL:

http://tftpd32.jounin.net

Follow the instructions on the website for installing and using the utility.

Translated Safety Warnings

For translated safety warnings, refer to the safety warning document that shipped with your access point or that is available on Cisco.com.

To browse to the document on Cisco.com, follow these steps:

Step 1 Click this link to the Cisco Wireless documentation home page:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

Step 2 Click **Cisco Aironet 1100 Series** listed under Access Points.

Step 3 Click **Install and Upgrade Guides**.

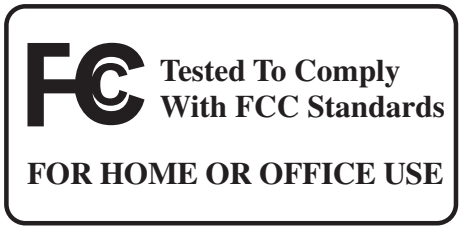
Step 4 Click **Safety Warnings for Cisco Aironet 1000, 1100, 1130AG, 1200, and 1240AG Series Access Points**.

Declarations of Conformity and Regulatory Information

This appendix provides declarations of conformity and regulatory information for the Cisco Aironet 1100 Series Access Points and the Cisco Aironet 1100 Series Cisco Aironet 1100 Series Lightweight Access Points.

This appendix contains the following sections:

Manufacturers Federal Communication Commission Declaration of Conformity Statement



Autonomous Access Point Models:

AIR-AP1120B-A-K9 or
AIR-AP1121G-A-K9

Lightweight Access Point Model:

AIR-LAP1121G-A-K9

FCC Certification number:

LDK 102042 (AIR-MPI350) or
LDK 102048 (AIR-MP21G-A-K9)

Manufacturer:

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

This device complies with Part 15 rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits of a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential environment. This equipment generates, uses, and radiates radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference. However, there is no guarantee that interference will not occur. If this equipment does cause interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician.

Caution The Part 15 radio device operates on a non-interference basis with other devices operating at this frequency. Any changes or modification to said product not expressly approved by Cisco could void the user's authority to operate this device.

VCCI Statement for Japan

Warning **This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.**

警告 VCCI 準拠クラスB機器（日本）
この装置は、情報処理装置等電波障害自主規制協議会（VCCI）の基準に基づくクラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをしてください。

Industry—Canada

Canadian Compliance Statement

This Class B Digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numerique de la classe B respecte les exigences du Reglement sur le material broilleur du Canada.

This device complies with Class B Limits of Industry Canada. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

The device is certified to the requirements of RSS-210 for 2.4-GHz spread spectrum devices. The use of this device in a system operating either partially or completely outdoors may require the user to obtain a license for the system according to the Canadian regulations. For further information, contact your local Industry Canada office.

European Community, Switzerland, Norway, Iceland, and Liechtenstein

Declaration of Conformity with Regard to the R&TTE Directive 1999/5/EC

Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales asi como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviski [Latvian]:	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.

121403

Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiele eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-ħtiġiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Margyar [Hungarian]:	Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.
Norsk [Norwegian]:	Dette utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]:	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.
Português [Portuguese]:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Slovensko [Slovenian]:	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.
Slovensky [Slovak]:	Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.
Suomi [Finnish]:	Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

121404

This device complies with the EMC requirements (EN 60601-1-2) of the Medical Directive 93/42/EEC.

This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

For the 1100 series access point, the following standards were applied:

- Radio: EN 300.328-1, EN 300.328-2
- EMC: EN 301 489-1, EN 301 489-17
- Safety: EN 60950

The following CE mark is affixed to the 1100 series equipment:

The above CE mark is required as of April 8, 2000 but might change in the future.

Note This equipment is intended to be used in all EU and EFTA countries. Outdoor use may be restricted to certain frequencies and/or may require a license for operation. For more details, contact Cisco Corporate Compliance.

Note Combinations of power levels and antennas resulting in a radiated power level of above 100 mW eirp are considered as not compliant with the above mentioned directive and are not allowed for use within the European community and countries that have adopted the European R&TTE directive 1999/5/EC and/or the CEPT recommendation Rec 70.03. For more details on legal combinations of power levels and antennas, contact Cisco Corporate Compliance.

Declaration of Conformity for RF Exposure

The radio module has been evaluated under FCC Bulletin OET 65C and found compliant to the requirements in CFR 47 Sections 2.1091, and 15.247 (b) (4) addressing RF Exposure from radio frequency devices. The access point should be installed more than 20 cm from your body or nearby persons.

Guidelines for Operating Cisco Aironet Access Points and Bridges in Japan

This section provides guidelines for avoiding interference when operating Cisco Aironet access points and bridges in Japan. These guidelines are provided in both Japanese and English.

Japanese Translation

この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）が運用されています。

1　この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認して下さい。

2　万一、この機器から移動体識別用の構内無線局に対して電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、下記連絡先にご連絡頂き、混信回避のための処置等(例えば、パーティションの設置など)についてご相談して下さい。

3　その他、この機器から移動体識別用の特定小電力無線局に対して電波干渉の事例が発生した場合など何かお困りのことが起きたときは、次の連絡先へお問い合わせ下さい。

連絡先：03-5549-6500

43768

English Translation

This equipment operates in the same frequency bandwidth as industrial, scientific, and medical devices such as microwave ovens and mobile object identification (RF-ID) systems (licensed premises radio stations and unlicensed specified low-power radio stations) used in factory production lines.

1. Before using this equipment, make sure that no premises radio stations or specified low-power radio stations of RF-ID are used in the vicinity.
2. If this equipment causes RF interference to a premises radio station of RF-ID, promptly change the frequency or stop using the device; contact the number below and ask for recommendations on avoiding radio interference, such as setting partitions.
3. If this equipment causes RF interference to a specified low-power radio station of RF-ID, contact the number below.

   Contact Number: 03-5549-6500

Administrative Rules for Cisco Aironet Access Points in Taiwan

This section provides administrative rules for operatingCisco Aironet access points inTaiwan. The rules are provided in both Chinese and English.

All Access Points

Chinese Translation

低功率電波輻射性電機管理辦法

第十四條　經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十七條　低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

95815

English Translation

Administrative Rules for Low-power Radio-Frequency Devices

Article 14

For those low-power radio-frequency devices that have already received a type-approval, companies, business units or users should not change its frequencies, increase its power or change its original features and functions.

Article 17

The operation of the low-power radio-frequency devices is subject to the conditions that no harmful interference is caused to aviation safety and authorized radio station; and if interference is caused, the user must stop operating the device immediately and can't re-operate it until the harmful interference is clear.

The authorized radio station means a radio-communication service operating in accordance with the Communication Act.

The operation of the low-power radio-frequency devices is subject to the interference caused by the operation of an authorized radio station, by another intentional or unintentional radiator, by industrial, scientific and medical (ISM) equipment, or by an incidental radiator.

Operation of Cisco Aironet Access Points in Brazil

This section contains special information for operation of Cisco Aironet access points in Brazil.

Access Point Models

AIR-AP1121G-A-K9
AIR-LAP1121G-A-K9

Regulatory Information

Figure B-1 contains Brazil regulatory information for the AIR-AP1121G-A-K9 and AIR-LAP1121G-A-K9 the access points.

Figure B-1 Brazil Regulatory Information

Portuguese Translation

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

English Translation

This equipment operates on a secondary basis and, consequently, must accept harmful interference, including from stations of the same kind, and may not cause harmful interference to systems operating on a primary basis.

Declaration of Conformity Statements

All the Declaration of Conformity statements related to this product can be found at the following URL:

http://www.ciscofax.com

Declaration of Conformity Statements for European Union Countries

The Declaration of Conformity statements for the European Union countries are listed below:

DECLARATION OF CONFORMITY

with regard to the R&TTE Directive 1999/5/EC & Medical Directive 93/42/EEC

according to EN 45014

Cisco Systems Inc.
170 West Tasman Drive
San Jose, CA 95134 - USA

Declare under our sole responsibility that the product,

Product: ***AIR-AP1120B-E-K9*** */ Wireless LAN Access Point (2,4 GHz version)*

Options included: ***AIR-MP20B-E-K9 or AIR-MPI350*** */ 2.4 GHz Mini PCI Radio Module*

Fulfils the essential requirements of Directives 1999/5/EC and 93/42/EEC.

The following standards were applied:

EMC	**EN 301.489-1: 2000-08; EN 301.489-17: 2000-09** **EN 60601-1-2: 1993**
Health & Safety	**EN60950: 1999**
Radio	**EN 300.328-1: 2001-12; EN 300.328-2: 2001-12**

The following conformity assessment procedures have been followed:

- Directive 1999/5/EC : procedure referred to in Article 10.4 and Annex III.
- Directive 93/42/EEC: procedure referred to in Article 11.5 and Annex VII.

The product carries the CE Mark: CE 0682 !

Date & Place of Issue: 3 April 2003 - Paris

Signature:

Frank Dewachter
Manager Corporate Compliance EMEA
11, rue Camille Desmoulins
92782, Issy Les Moulineaux Cedex 9 France

DofC 234998rev1

DECLARATION OF CONFORMITY

with regard to the R&TTE Directive 1999/5/EC

according to EN 45014

Cisco Systems Inc.
170 West Tasman Drive
San Jose, CA 95134
USA

Declare under our sole responsibility that the product,

AIR-AP1121G-E-K9 */ 2.4 GHz 54 Mbps Wireless LAN Access Point*

Options included*:* ***AIR-MP21G-E-K9*** */ 2.4 GHz Mini PCI Radio Module*

Fulfils the essential requirements of Directive 1999/5/EC.

The following standards were applied:

EMC	**EN 301 489-1: 2002-08; EN 301 489-17: 2002-04**
Health & Safety	**EN60950: 2000**
Radio	**EN 300 328-2: 2001-12; EN 300 328: 2003-04**

The conformity assessment procedure referred to in Article 10.4 and Annex III of Directive 1999/5/EC has been followed.

The product carries the CE Mark:

Date & Place of Issue: 15 September 2003 - Paris

Signature:

Frank Dewachter
Manager Corporate Compliance EMEA
11, rue Camille Desmoulins
92782, Issy Les Moulineaux Cedex 9 France

DofC 323387

DECLARATION OF CONFORMITY

with regard to the R&TTE Directive 1999/5/EC

according to EN 45014

Cisco Systems Inc.
170 West Tasman Drive
San Jose, CA 95134
USA

Declare under our sole responsibility that the product,

AIR-MP21G-E-K9 */ 2.4 GHz 54 Mbps Mini PCI Radio Module*

Fulfils the essential requirements of Directive 1999/5/EC.

The following standards were applied:

EMC	**EN 301 489-1: 2002-08; EN 301 489-17: 2002-04**
Health & Safety	**EN60950: 2000**
Radio	**EN 300 328-2: 2001-12; EN 300 328: 2003-04**

The conformity assessment procedure referred to in Article 10.4 and Annex III of Directive 1999/5/EC has been followed.

The product carries the CE Mark:

Date & Place of Issue: 15 September 2003 - Paris

Signature:

Frank Dewachter
Manager Corporate Compliance EMEA
11, rue Camille Desmoulins
92782, Issy Les Moulineaux Cedex 9 France

DofC 323389

DECLARATION OF CONFORMITY

with regard to the R&TTE Directive 1999/5/EC

according to EN 45014

Cisco Systems Inc.
170 West Tasman Drive
San Jose, CA 95134
USA

Declare under our sole responsibility that the product,

AIR-MPI 350 / 2.4 GHz 11 Mbps Mini PCI Embedded Adapter
Variants : AIR-MPI 352, AIR-MP20B-E-K9

Fulfils the essential requirements of Directive 1999/5/EC.

The following standards were applied:

EMC	**EN 301.489-1: 2000-08; EN 301.489-17: 2000-09**
Health & Safety	**EN60950: 1992+A1+A2+A3+A4**
Radio	**EN 300.328-1 and -2: 2000-7**

The conformity assessment procedure referred to in Article 10.4 and Annex III of Directive 1999/5/EC has been followed.

The product carries the CE Mark:

Date & Place of Issue: 1 April 2002 - Paris

Signature:

Frank Dewachter
Manager Corporate Compliance EMEA
11, rue Camille Desmoulins
92782, Issy Les Moulineaux Cedex 9 France

DofC 136186rev1

Access Point Specifications

This appendix provides technical specifications for the 1100 series access point. Table C-1 lists the technical specifications for the access point.

Table C-1 Access Point Specifications

Category	Specifications
Physical	
Size	4.1 in. W x 1.5 in. D x 8.1 in. H 10.4 cm W x 3.8 cm D x 20.6 cm H
Status Indicators	Three indicators on the top panel: • Ethernet traffic • Status • Radio traffic
Connectors	End panel (left to right): RJ-45 connector for 10/100 BASE-T Ethernet connections; power connector (for plug-in AC power module).
Input Voltage	48 VDC nominal. Operational up to 60 VDC. Voltage higher than 60 VDC can damage the unit.
Input Power	With IEEE 802.11b-compliant radio: 4.75 W With IEEE 802.11g-compliant radio: 4.75 W (typical)
Operating Temperature	32 to 104°F (0 to 40°C) for the access point 32 to 104°F (0 to 40°C) for the power injector
Storage Temperature	–13 to 158°F (–25 to 70°C) for access point
Weight	10.5 oz (297g) with 2.4-GHz radio

Table C-1 Access Point Specifications (continued)

Category	Specifications
Radio	**2.4-GHz Radio**
Power Output	Autonomous access point: With IEEE 802.11b-compliant radio: 100, 50, 30, 20, 5, or 1 mW (at 1, 2, 5.5, and 11Mbps) With IEEE 802.11g-compliant radio: 100, 50, 30, 20, 10, 5, or 1 mW (at 1, 2, 5.5 and 11 Mbps) 50, 30, 20, 10, 5, or 1 mW (at 6, 9, 12, 18, 24, 48, and 54 Mbps) Lightweight access point: With IEEE 802.11g-compliant radio: 100, 50, 25, 12, 6, 3, 2, 1 mW (at 1, 2, 5.5 and 11 Mbps) 50, 25, 12, 6, 3, 2, 1 mW (at 6, 9, 12, 18, 24, 48, and 54 Mbps) (Depending on the regulatory domain in which the access point is installed)
Frequency	2.400 to 2.497 GHz (Depending on the regulatory domain in which the access point is installed)
Modulation	IEEE 802.11b-compliant radio: Complementary Code Keying (CCK) IEEE 802.11g-compliant radio: Orthogonal Frequency Division Multiplex (OFDM)
Data rates	IEEE 802.11b-compliant radio: 1, 2, 5.5, and 11 Mbps IEEE 802.11g-compliant radio: 1, 2, 5.5, and 11 Mbps 6, 9, 12, 18, 24, 36, 48, and 54 Mbps

Table C-1 Access Point Specifications (continued)

Category	Specifications
Typical Range	Indoor (across office cubicle walls): IEEE 802.11b-compliant radio: (maximum output power) 400 ft (121.9 m) at 1 Mbps 150 ft (45.7 m) at 11 Mbps IEEE 802.11g-compliant radio: (maximum output power) 410 ft (125.0 m) at 1 Mbps 270 ft (82.3 m) at 2 Mbps 220 ft (67.1 m) at 5.5 Mbps 160 ft (48.8 m) at 11 Mbps 300 ft (91.4 m) at 6 Mbps 210 ft (67.1 m) at 12 Mbps 180 ft (54.9 m) at 18 Mbps 90 ft (27.4 m) at 54 Mbps Outdoor: IEEE 802.11b-compliant radio: (maximum output power) 2000 ft (609.6 m) at 1 Mbps 800 ft (243.8 m) at 11 Mbps IEEE 802.11g-compliant radio: (maximum output power) 2000 ft (609.6 m) at 1 Mbps 1000 ft (304.8 m) at 11 Mbps 1300 ft (396.2 m) at 6 Mbps 600 ft (182.9 m) at 18 Mbps 250 ft (76.2 m) at 54 Mbps **Note** Using 2.2dBi antennas at the access point and the client adapter.
Antenna	A diversity system with two integrated 2.2 dBi dipole antennas.
Compliance	The 1100 series access point provides adequate fire resistance and low smoke-producing characteristics suitable for operation in a building's environmental air space, such as above suspended ceilings, in accordance with Section 300-22 (C) of the National Electrical Code (NEC) and Sections 2-128, 12-010(3) and 12-100 of the Canadian Electrical Code, Part 1, C22.1. **Caution** Only the fiber-optic power injector (AIR-PWRINJ-FIB) has been tested to UL 2043 for operation in a building's environmental air space; no other power injectors or power modules have been tested to UL 2043 and they should not be placed in a building's environmental air space, such as above suspended ceilings.

Table C-1 Access Point Specifications (continued)

Category	Specifications
Safety	Designed to meet: • UL 1950 • CSA 22.2 No. 950-95 • IEC 60950 • EN 60950
Radio Approvals	IEEE 802.11b-compliant radio: FCC Part 15.247 Japan ARIB-STD-33B EN 300.328 IEEE 802.11g-compliant radio: FCC Parts 15.247, 15.205, 15.209 Canada RSS-210 Japan ARIB-STD-33B Japan ARIB-STD-66 Europe EN-300.328
EMI and Susceptibility	FCC Part 15.107 and 15.109 Class B ICES-003 Class B (Canada) AS/NZS 3548 Class B VCCI Class B EN 60601-1-2:2001 EN 301.489-1 EN 301.489-17
RF Exposure	OET-65C RSS-102 ANSI C95.1

Channels and Maximum Power Levels

For channel and maximum power level settings, refer to the *Channels and Maximum Power Settings for Cisco Aironet Autonomous Access Points and Bridges* or the *Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points and Bridges* documents available on the Cisco Wireless documentation page of Cisco.com.

To browse to the documents, follow these steps:

Step 1 Click this link to the Cisco Wireless documentation home page:

http://www.cisco.com/en/US/products/hw/wireless/tsd_products_support_category_home.html

Step 2 Click **Cisco Aironet 1100 Series** listed under Access Points.

Step 3 Click **Install and Upgrade Guides**.

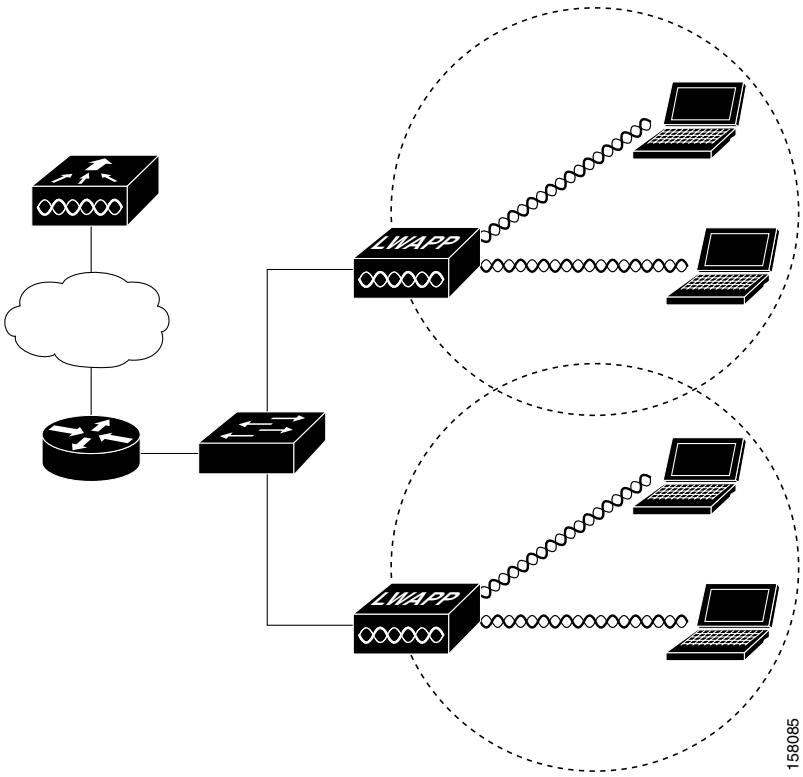
Step 4 Click **Channels and Maximum Power Settings for Cisco Aironet Autonomous Access Points and Bridges** or the **Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points and Bridges**.

Priming Lightweight Access Points Prior to Deployment

This section describes an optional procedure designed to prime or stage your lightweight access points in a convenient location rather than after they are installed in possibly difficult to reach locations. This process can be used when a DHCP server is not reachable by your deployed access point and it helps limit potential installation problems to primarily Ethernet and power areas.

Figure E-1 illustrates a typical priming configuration for your lightweight access points.

Figure E-1 Typical Lightweight Access Point Priming Configuration



Before deploying your lightweight access points to their final locations, follow these steps to prime your access points:

Step 1 In a Layer 3 environment, ensure a DHCP server (typically on your switch) is enabled on the same subnet as your lightweight access points. The access points receives its IP address and controller information using DHCP Option 43.

The lightweight access point must be able to find the IP address of the controller. This can be accomplished using DHCP, DNS, OTAP, or IP subnet broadcast. This guide describes the DHCP method to convey the controller IP address. For other methods, refer to the product documentation. See also the "Using DHCP Option 43" section on page 6-2 for more information.

Note For a Layer 3 access point on a different subnet than the controller, ensure the route to the controller has destination UDP ports 12222 and 12223 open for LWAPP communications. Ensure that the routes to the primary, secondary, and tertiary controllers allow IP packet fragments.

Step 2 Ensure that your controller is connected to a switch trunk port.

Step 3 Configure the controller in LWAPP Layer 3 mode and ensure its DS Port is connected to the switch. Use the CLI, web-browser interface, or Cisco WCS procedures as described in the appropriate controller guide.

a. In multi-controller environments, You can set one controller's DS port to **Master** (you can use the *config network master-base disable* CLI command or you can use the controller GUI*)* so that new lightweight access points always associate with it. You can use the *show network config* CLI command to determine if the controller DS port is the master.

All lightweight access points associate to the master controller. From one location, you can configure lightweight access point settings such as primary, secondary, and tertiary controllers. This allows you to redistribute your lightweight access points to other controllers on the network.

You can also use a Cisco WCS server to control, configure, and redistribute all your lightweight access points from a single location.

Step 4 Apply power to the access points:

a. Connect your lightweight access points to untagged access ports on your POE capable switch. You can optionally use power modules or power injectors to power your access points.

b. After you power up the lightweight access point, it begins a power-up sequence that you can check by observing the access point LEDs. All LEDs blink sequentially back and forth, indicating that the access point is trying to find a controller.

Note If the access point remains in this mode for more than 5 minutes, the access point is unable to find the master controller. Check the connection between the access point and the controller and ensure they are on the same subnet.

c. If the lightweight access point shuts down (all LEDs off), check to ensure that sufficient power is available.

d. When the lightweight access point associates with the controller, if the access point code version differs from the controller code version, the access point downloads the operating system code from the controller. All the access point LEDs blink simultaneously during the download.

Step 5 If the operating system download is successful, the access point reboots. Normal operation is indicated when the radio LED is blinking to indicate radio activity.

Step 6 Use controller CLI, controller GUI, or Cisco WCS to configure the lightweight access point with primary, secondary, and tertiary controller names.

Step 7 If the lightweight access point is in a Controller Mobility Group, use the controller CLI, controller GUI, or Cisco WCS to configure the Controller Mobility Group name.

Step 8 Use controller CLI, controller GUI, or Cisco WCS to configure the lightweight access point-specific 802.11a, 802.11b, and 802.11g network settings.

Step 9 If the configuration priming was successful, the radio LED is blinking to indicate normal operation.

Step 10 Repeat Steps 4 to 9 for each lightweight access point.

When you successfully complete the configuration priming of all your lightweight access points, ensure Master setting is disabled on your controller. You can begin deploying the access points to their final destinations (refer to the "Deploying the Access Points on the Wireless Network" section on page 2-5).

Configuring DHCP Option 43 for Lightweight Access Points

This appendix describes the steps needed to configure DHCP Option 43 for use with Cisco Aironet lightweight access points. This appendix contains these sections:

Overview

This section contains a DHCP Option 43 configuration example on the embedded Cisco IOS DHCP server for use with Cisco Aironet lightweight access points. For instructions on configuring DHCP Option 43 on Microsoft, Sun Solaris, Linux, and Lucent QIP DHCP servers, consult the document at this URL:

http://www.cisco.com/en/US/tech/tk722/tk809/technologies_configuration_example09186a00808714fe.shtml

For other DHCP server implementations, consult the DHCP server documentation for instructions on configuring DHCP Option 43. In Option 43, you should use the IP address of the controller management interface.

Note DHCP Option 43 is limited to one access point type per DHCP pool. You must configure a separate DHCP pool for each access point type.

Cisco Aironet 1000 and 1500 series access points use a comma-separated string format for DHCP Option 43. Other Cisco Aironet lightweight access points use the type-length-value (TLV) format for DHCP Option 43. DHCP servers must be programmed to return the option based on the access point's DHCP Vendor Class Identifier (VCI) string (DHCP Option 60). The VCI strings for Cisco access points capable of operating in lightweight mode are listed in Table F-1:

Table F-1 Lightweight Access Point VCI Strings

Lightweight Access Point	Vendor Class Identifier (VCI)
Cisco Aironet 1000 series	Airespace.AP1200
Cisco Aironet 1100 series	Cisco AP c1100
Cisco Aironet 1130 series	Cisco AP c1130
Cisco Aironet 1200 series	Cisco AP c1200
Cisco Aironet 1240 series	Cisco AP c1240
Cisco Aironet 1300 series	Cisco AP c1300
Cisco Aironet 1500 series	Cisco AP.LAP1510?

The format of the TLV block for 1100, 1130, 1200, 1240, 1250, and 1300 series lightweight access points is listed below:

- Type: 0xf1 (decimal 241)
- Length: Number of controller IP addresses * 4
- Value: List of WLC management interfaces

Configuring Option 43 for 1000 Series Access Points

To configure DHCP Option 43 for Cisco 1000 series lightweight access points in the embedded Cisco IOS DHCP server, follow these steps:

Step 1 Enter configuration mode at the Cisco IOS command line interface (CLI).

Step 2 Create the DHCP pool, including the necessary parameters such as default router and name server. A DHCP scope example is as follows:

```
ip dhcp pool <pool name>
network <IP Network> <Netmask>
default-router <Default router>
dns-server <DNS Server>

Where:
    <pool name> is the name of the DHCP pool, such as AP1000
    <IP Network> is the network IP address where the controller resides, such as 10.0.15.1
    <Netmask> is the subnet mask, such as 255.255.255.0
    <Default router> is the IP address of the default router, such as 10.0.0.1
    <DNS Server> is the IP address of the DNS server, such as 10.0.10.2
```

Step 3 Add the option 60 line using the following syntax:

```
option 60 ascii "Airespace.AP1200"
```

The quotation marks must be included.

Step 4 Add the option 43 line using the following syntax:

```
option 43 ascii "Comma Separated IP Address List"
```

For example, if you are configuring option 43 for Cisco 1000 series access points using the controller IP addresses 10.126.126.2 and 10.127.127.2, add the following line to the DHCP pool in the Cisco IOS CLI:

```
option 43 ascii "10.126.126.2,10.127.127.2"
```

The quotation marks must be included.

Configuring Option 43 for 1100, 1130, 1200, 1240, and 1300 Series Access Points

To configure DHCP Option 43 for Cisco Aironet 1100, 1130, 1200, 1240, and 1300 series lightweight access points in the embedded Cisco IOS DHCP server, follow these steps:

Step 1 Enter configuration mode at the Cisco IOS CLI.

Step 2 Create the DHCP pool, including the necessary parameters such as default router and name server. A DHCP scope example is as follows:

```
ip dhcp pool <pool name>
network <IP Network> <Netmask>
default-router <Default router>
dns-server <DNS Server>

Where:
    <pool name> is the name of the DHCP pool, such as AP1240
    <IP Network> is the network IP address where the controller resides, such as 10.0.15.1
    <Netmask> is the subnet mask, such as 255.255.255.0
    <Default router> is the IP address of the default router, such as 10.0.0.1
    <DNS Server> is the IP address of the DNS server, such as 10.0.10.2
```

Step 3 Add the option 60 line using the following syntax:

```
option 60 ascii "VCI string"
```

For the *VCI string*, use the value from Table F-1. The quotation marks must be included.

Step 4 Add the option 43 line using the following syntax:

```
option 43 hex <hex string>
```

The *hex string* is assembled by concatenating the TLV values shown below:

Type + *Length* + *Value*

Type is always *f1(hex)*. *Length* is the number of controller management IP addresses times 4 in hex. *Value* is the IP address of the controller listed sequentially in hex.

For example, suppose that there are two controllers with management interface IP addresses, 10.126.126.2 and 10.127.127.2. The type is *f1(hex)*. The length is *2 * 4 = 8 = 08 (hex)*. The IP addresses translate to *0a7e7e02* and *0a7f7f02*. Assembling the string then yields *f1080a7e7e020a7f7f02*. The resulting Cisco IOS command added to the DHCP scope is listed below:

```
option 43 hex f1080a7e7e020a7f7f02
```

802.11 The IEEE standard that specifies carrier sense media access control and physical layer specifications for 1- and 2-megabit-per-second (Mbps) wireless LANs operating in the 2.4-GHz band.

802.11a The IEEE standard that specifies carrier sense media access control and physical layer specifications for wireless LANs operating in the 5-GHz frequency band.

802.11b The IEEE standard that specifies carrier sense media access control and physical layer specifications for 5.5- and 11-Mbps wireless LANs operating in the 2.4-GHz frequency band.

A

access point A wireless LAN data transceiver that uses radio waves to connect a wired network with wireless stations.

ad hoc network A wireless network composed of stations without Access Points.

antenna gain The gain of an antenna is a measure of the antenna's ability to direct or focus radio energy over a region of space. High gain antennas have a more focused radiation pattern in a specific direction.

associated A station is configured properly to allow it to wirelessly communicate with an Access Point.

B

beacon A wireless LAN packet that signals the availability and presence of the wireless device. Beacon packets are sent by access points and base stations; however, client radio cards send beacons when operating in computer to computer (Ad Hoc) mode.

BOOTP Boot Protocol. A protocol used for the static assignment of IP addresses to devices on the network.

BPSK A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 1 Mbps.

broadcast packet A single data message (packet) sent to all addresses on the same subnet.

C

CCK Complementary code keying. A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 5.5 and 11 Mbps.

cell The area of radio range or coverage in which the wireless devices can communicate with the base station. The size of the cell depends upon the speed of the transmission, the type of antenna used, and the physical environment, as well as other factors.

client A radio device that uses the services of an Access Point to communicate wirelessly with other devices on a local area network.

CSMA Carrier sense multiple access. A wireless LAN media access method specified by the IEEE 802.11 specification.

D

data rates The range of data transmission rates supported by a device. Data rates are measured in megabits per second (Mbps).

dBi A ratio of decibels to an isotropic antenna that is commonly used to measure antenna gain. The greater the dBi value, the higher the gain, and the more acute the angle of coverage.

DHCP Dynamic host configuration protocol. A protocol available with many operating systems that automatically issues IP addresses within a specified range to devices on the network. The device retains the assigned address for a specific administrator-defined period.

dipole A type of low-gain (2.2-dBi) antenna consisting of two (often internal) elements.

domain name The text name that refers to a grouping of networks or network resources based on organization-type or geography; for example: name.com—commercial; name.edu—educational; name.gov—government; ISPname.net—network provider (such as an ISP); name.ar—Argentina; name.au—Australia; and so on.

DNS Domain Name System server. A server that translates text names into IP addresses. The server maintains a database of host alphanumeric names and their corresponding IP addresses.

DSSS Direct sequence spread spectrum. A type of spread spectrum radio transmission that spreads its signal continuously over a wide frequency band.

E

EAP Extensible Authentication Protocol. An optional IEEE 802.1x security feature ideal for organizations with a large user base and access to an EAP-enabled Remote Authentication Dial-In User Service (RADIUS) server.

Ethernet The most widely used wired local area network. Ethernet uses carrier sense multiple access (CSMA) to allow computers to share a network and operates at 10, 100, or 1000 Mbps, depending on the physical layer used.

F

file server A repository for files so that a local area network can share files, mail, and programs.

firmware Software that is programmed on a memory chip.

G

gateway A device that connects two otherwise incompatible networks together.

GHz Gigahertz. One billion cycles per second. A unit of measure for frequency.

I

IEEE Institute of Electrical and Electronic Engineers. A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications.

infrastructure The wired Ethernet network.

IP Address The Internet Protocol (IP) address of a station.

IP subnet mask The number used to identify the IP subnetwork, indicating whether the IP address can be recognized on the LAN or if it must be reached through a gateway. This number is expressed in a form similar to an IP address; for example: 255.255.255.0.

isotropic An antenna that radiates its signal in a spherical pattern.

M

MAC Media Access Control address. A unique 48-bit number used in Ethernet data packets to identify an Ethernet device, such as an access point or your client adapter.

modulation Any of several techniques for combining user information with a transmitter's carrier signal.

multipath The echoes created as a radio signal bounces off of physical objects.

multicast packet A single data message (packet) sent to multiple addresses.

O

omni-directional This typically refers to a primarily circular antenna radiation pattern.

orthogonal Frequency Division Multiplex (OFDM) A modulation technique used by IEEE 802.11a-compliant wireless LANs for transmission at 6, 9, 12, 18, 24, 36, 48, and 54 Mbps.

P

packet A basic message unit for communication across a network. A packet usually includes routing information, data, and sometimes error detection information.

Q

Quadruple Phase Shift Keying A modulation technique used by IEEE 802.11b-compliant wireless LANs for transmission at 2 Mbps.

R

range A linear measure of the distance that a transmitter can send a signal.

receiver sensitivity A measurement of the weakest signal a receiver can receive and still correctly translate it into data.

RF Radio frequency. A generic term for radio-based technology.

roaming A feature of some Access Points that allows users to move through a facility while maintaining an unbroken connection to the LAN.

RP-TNC A connector type unique to Cisco Aironet radios and antennas. Part 15.203 of the FCC rules covering spread spectrum devices limits the types of antennas that may be used with transmission equipment. In compliance with this rule, Cisco Aironet, like all other wireless LAN providers, equips its radios and antennas with a unique connector to prevent attachment of non-approved antennas to radios.

S

spread spectrum A radio transmission technology that spreads the user information over a much wider bandwidth than otherwise required in order to gain benefits such as improved interference tolerance and unlicensed operation.

SSID Service Set Identifier (also referred to as Radio Network Name). A unique identifier used to identify a radio network and which stations must use to be able to communicate with each other or to an access point. The SSID can be any alphanumeric entry up to a maximum of 32 characters.

T

transmit power The power level of radio transmission.

U

UNII Unlicensed National Information Infrastructure—regulations for UNII devices operating in the 5.15 to 5.35 GHz and 5.725 to 5.825 GHz frequency bands.

UNII-1 Regulations for UNII devices operating in the 5.15 to 5.25 GHz frequency band.

UNII-2 Regulations for UNII devices operating in the 5.25 to 5.35 GHz frequency band.

UNII-3 Regulations for UNII devices operating in the 5.725 to 5.825 GHz frequency band.

unicast packet A single data message (packet) sent to a specific IP address.

W

WEP Wired Equivalent Privacy. An optional security mechanism defined within the IEEE 802.11 standard designed to make the link integrity of wireless devices equal to that of a cable.

workstation A computing device with an installed client adapter.

O

P

R

S

T

U

V

W